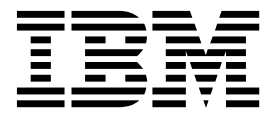


IBM Security QRadar  
Version 7.2.6

*API Guide*



**Note**

Before using this information and the product that it supports, read the information in “Notices” on page 619.

**Product information**

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

© Copyright IBM Corporation 2014, 2015.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Chapter 1. What's new for developers in RESTful APIs in QRadar V7.2.6 . . . . .</b>	<b>1</b>
New endpoints in more detail . . . . .	1
Deprecated endpoints in more detail . . . . .	4
<b>Chapter 2. RESTful API overview . . . . .</b>	<b>5</b>
Filter syntax . . . . .	8
Sort syntax . . . . .	12
Paging syntax . . . . .	12
API error messages . . . . .	13
Cross-origin resource sharing . . . . .	16
<b>Chapter 3. API command-line client . . . . .</b>	<b>17</b>
<b>Chapter 4. Accessing the interactive API documentation page . . . . .</b>	<b>19</b>
<b>Chapter 5. REST API V5.0 References . . . . .</b>	<b>21</b>
Analytics endpoints . . . . .	21
GET /analytics/custom_actions/actions . . . . .	21
POST /analytics/custom_actions/actions . . . . .	22
GET /analytics/custom_actions/interpreters . . . . .	24
GET /analytics/custom_actions/interpreters/{interpreter_id}. . . . .	26
GET /analytics/custom_actions/scripts . . . . .	27
POST /analytics/custom_actions/scripts . . . . .	28
GET /analytics/custom_actions/actions/{action_id} . . . . .	29
POST /analytics/custom_actions/actions/{action_id} . . . . .	30
DELETE /analytics/custom_actions/actions/{action_id} . . . . .	32
GET /analytics/custom_actions/scripts/{script_id} . . . . .	33
POST /analytics/custom_actions/scripts/{script_id}. . . . .	34
DELETE /analytics/custom_actions/scripts/{script_id}. . . . .	35
Ariel endpoints . . . . .	36
GET /ariel/databases . . . . .	36
GET /ariel/databases/{database_name} . . . . .	37
GET /ariel/searches . . . . .	38
POST /ariel/searches . . . . .	39
GET /ariel/searches/{search_id} . . . . .	40
POST /ariel/searches/{search_id} . . . . .	42
DELETE /ariel/searches/{search_id} . . . . .	43
GET /ariel/searches/{search_id}/results. . . . .	45
Asset model endpoints . . . . .	46
GET /asset_model/assets. . . . .	46
POST /asset_model/assets/{asset_id} . . . . .	47
GET /asset_model/properties . . . . .	48
GET /asset_model/saved_searches . . . . .	49
GET /asset_model/saved_searches/{saved_search_id}/results . . . . .	51
Authentication endpoints. . . . .	52
POST /auth/logout . . . . .	53
Configuration endpoints . . . . .	53
GET /config/domain_management/domains . . . . .	53
POST /config/domain_management/domains . . . . .	55
GET /config/domain_management/domains/{domain_id} . . . . .	56
POST /config/domain_management/domains/{domain_id} . . . . .	58
DELETE /config/domain_management/domains/{domain_id} . . . . .	59
GET /config/access/tenant_management/tenants . . . . .	61
POST /config/access/tenant_management/tenants . . . . .	62

GET /config/access/tenant_management/tenants/{tenant_id}	63
POST /config/access/tenant_management/tenants/{tenant_id}	64
DELETE /config/access/tenant_management/tenants/{tenant_id}	65
GET /config/extension_management/extensions	66
POST /config/extension_management/extensions	69
GET /config/extension_management/extensions/{extension_id}	71
POST /config/extension_management/extensions/{extension_id}	73
DELETE /config/extension_management/extensions/{extension_id}	75
GET /config/extension_management/extensions_task_status/{status_id}	77
GET /config/extension_management/extensions_task_status/{status_id}/results	78
GUI application framework endpoints	80
GET /gui_app_framework/application_creation_task	80
POST /gui_app_framework/application_creation_task	81
GET /gui_app_framework/application_creation_task/{application_id}	82
POST /gui_app_framework/application_creation_task/{application_id}	83
GET /gui_app_framework/applications	84
GET /gui_app_framework/applications/{application_id}	86
POST /gui_app_framework/applications/{application_id}	89
DELETE /gui_app_framework/applications/{application_id}	92
Help endpoints	92
GET /help/capabilities	92
QRadar Vulnerability Manager endpoints	95
GET /qvm/assets	95
GET /qvm/filters	95
GET /qvm/network	96
GET /qvm/openservices	97
GET /qvm/savedsearches	97
POST /qvm/tickets/assign	98
GET /qvm/vulninstances	99
GET /qvm/vulns	99
Reference data endpoints	100
GET /reference_data/map_of_sets	100
POST /reference_data/map_of_sets	102
GET /reference_data/map_of_sets/{name}	103
POST /reference_data/map_of_sets/{name}	105
DELETE /reference_data/map_of_sets/{name}	106
GET /reference_data/map_of_sets/{name}/dependents	108
DELETE /reference_data/map_of_sets/{name}/value/{key}	110
GET /reference_data/maps	111
POST /reference_data/maps	112
GET /reference_data/maps/{name}	114
POST /reference_data/maps/{name}	116
DELETE /reference_data/maps/{name}	117
GET /reference_data/maps/{name}/dependents	119
DELETE /reference_data/maps/{name}/value/{key}	120
GET /reference_data/sets	122
POST /reference_data/sets	123
GET /reference_data/sets/{name}	124
POST /reference_data/sets/{name}	126
DELETE /reference_data/sets/{name}	127
GET /reference_data/sets/{name}/dependents	129
DELETE /reference_data/sets/{name}/value/{value}	130
POST /reference_data/sets/bulk_load/{name}	132
GET /reference_data/tables	133
POST /reference_data/tables	134
GET /reference_data/tables/{name}	135
POST /reference_data/tables/{name}	137
DELETE /reference_data/tables/{name}	138
GET /reference_data/tables/{name}/dependents	140
DELETE /reference_data/tables/{name}/value/{outer_key}/{inner_key}	142
Scanner endpoints	144

GET /scanner/profiles . . . . .	144
POST /scanner/profiles/create . . . . .	144
POST /scanner/profiles/start . . . . .	145
GET /scanner/scanprofiles . . . . .	146
POST /scanner/scanprofiles . . . . .	147
GET /scanner/scanprofiles/{profileid} . . . . .	148
POST /scanner/scanprofiles/{profileid} . . . . .	150
DELETE /scanner/scanprofiles/{profileid} . . . . .	151
POST /scanner/scanprofiles/{profileid}/start . . . . .	151
SIEM endpoints . . . . .	152
GET /siem/local_destination_addresses . . . . .	152
GET /siem/local_destination_addresses/{local_destination_address_id} . . . . .	154
GET /siem/offense_closing_reasons . . . . .	156
POST /siem/offense_closing_reasons . . . . .	157
GET /siem/offense_closing_reasons/{closing_reason_id} . . . . .	158
GET /siem/offenses . . . . .	159
GET /siem/offenses/{offense_id} . . . . .	162
POST /siem/offenses/{offense_id} . . . . .	166
GET /siem/offenses/{offense_id}/notes . . . . .	169
POST /siem/offenses/{offense_id}/notes . . . . .	171
GET /siem/offenses/{offense_id}/notes/{note_id} . . . . .	172
GET /siem/source_addresses . . . . .	173
GET /siem/source_addresses/{source_address_id} . . . . .	174
System endpoints . . . . .	176
GET /system/servers . . . . .	176
GET /system/servers/{server_id} . . . . .	177
POST /system/servers/{server_id} . . . . .	178
GET /system/servers/{server_id}/firewall_rules . . . . .	179
PUT /system/servers/{server_id}/firewall_rules . . . . .	181
GET /system/servers/{server_id}/network_interfaces/ethernet . . . . .	182
POST /system/servers/{server_id}/network_interfaces/ethernet/{device_name} . . . . .	184
GET /system/servers/{server_id}/network_interfaces/bonded . . . . .	186
POST /system/servers/{server_id}/network_interfaces/bonded/{device_name} . . . . .	189
<b>Chapter 6. Previous REST API versions . . . . .</b>	<b>193</b>
REST API V4.0 References . . . . .	193
Ariel endpoints. . . . .	193
GET /ariel/databases . . . . .	193
GET /ariel/databases/{database_name} . . . . .	194
GET /ariel/searches . . . . .	195
POST /ariel/searches. . . . .	196
GET /ariel/searches/{search_id} . . . . .	197
POST /ariel/searches/{search_id} . . . . .	199
DELETE /ariel/searches/{search_id} . . . . .	200
GET /ariel/searches/{search_id}/results . . . . .	202
Asset model endpoints . . . . .	203
GET /asset_model/assets . . . . .	203
POST /asset_model/assets/{asset_id} . . . . .	204
GET /asset_model/properties . . . . .	205
GET /asset_model/saved_searches . . . . .	206
GET /asset_model/saved_searches/{saved_search_id}/results . . . . .	208
Authentication endpoints . . . . .	209
POST /auth/logout . . . . .	210
Help endpoints. . . . .	210
GET /help/capabilities . . . . .	210
QRadar Vulnerability Manager endpoints . . . . .	212
GET /qvm/assets . . . . .	212
GET /qvm/filters . . . . .	213
GET /qvm/network . . . . .	214
GET /qvm/openservices . . . . .	214
GET /qvm/savedsearches . . . . .	215

POST /qvm/tickets/assign . . . . .	216
GET /qvm/vulninstances . . . . .	217
GET /qvm/vulns . . . . .	217
Reference data endpoints . . . . .	218
GET /reference_data/map_of_sets . . . . .	218
DELETE /reference_data/map_of_sets/{name} . . . . .	219
GET /reference_data/map_of_sets/{name} . . . . .	221
DELETE /reference_data/map_of_sets/{name}/{key} . . . . .	222
POST /reference_data/map_of_sets/{name} . . . . .	224
POST /reference_data/map_of_sets . . . . .	225
GET /reference_data/maps . . . . .	226
DELETE /reference_data/maps/{name} . . . . .	228
GET /reference_data/maps/{name} . . . . .	229
DELETE /reference_data/maps/{name}/{key} . . . . .	230
POST /reference_data/maps/{name} . . . . .	232
POST /reference_data/maps . . . . .	233
POST /reference_data/sets/bulk_load/{name} . . . . .	234
GET /reference_data/sets . . . . .	236
DELETE /reference_data/sets/{name} . . . . .	237
GET /reference_data/sets/{name} . . . . .	238
POST /reference_data/sets/{name} . . . . .	239
DELETE /reference_data/sets/{name}/{value} . . . . .	241
POST /reference_data/sets . . . . .	242
GET /reference_data/tables . . . . .	243
DELETE /reference_data/tables/{name} . . . . .	245
GET /reference_data/tables/{name} . . . . .	246
DELETE /reference_data/tables/{name}/{outer_key}/{inner_key} . . . . .	247
POST /reference_data/tables/{name} . . . . .	249
POST /reference_data/tables . . . . .	250
Scanner endpoints . . . . .	252
GET /scanner/profiles . . . . .	252
POST /scanner/profiles/create . . . . .	252
POST /scanner/profiles/start . . . . .	253
GET /scanner/scanprofiles . . . . .	254
POST /scanner/scanprofiles . . . . .	256
GET /scanner/scanprofiles/{profileid} . . . . .	256
POST /scanner/scanprofiles/{profileid} . . . . .	258
DELETE /scanner/scanprofiles/{profileid} . . . . .	259
POST /scanner/scanprofiles/{profileid}/start . . . . .	259
SIEM endpoints . . . . .	260
GET /siem/local_destination_addresses . . . . .	260
GET /siem/local_destination_addresses/{local_destination_address_id} . . . . .	262
GET /siem/offense_closing_reasons . . . . .	263
POST /siem/offense_closing_reasons . . . . .	265
GET /siem/offense_closing_reasons/{closing_reason_id} . . . . .	266
GET /siem/offenses . . . . .	267
GET /siem/offenses/{offense_id} . . . . .	270
POST /siem/offenses/{offense_id} . . . . .	273
GET /siem/offenses/{offense_id}/notes . . . . .	277
POST /siem/offenses/{offense_id}/notes . . . . .	278
GET /siem/offenses/{offense_id}/notes/{note_id} . . . . .	279
GET /siem/source_addresses . . . . .	280
GET /siem/source_addresses/{source_address_id} . . . . .	282
REST API V3.1 References . . . . .	283
Ariel endpoints . . . . .	283
GET /ariel/databases DEPRECATED . . . . .	283
GET /ariel/databases/{database_name} DEPRECATED . . . . .	284
GET /ariel/searches DEPRECATED . . . . .	285
POST /ariel/searches DEPRECATED . . . . .	286
GET /ariel/searches/{search_id} DEPRECATED . . . . .	288
POST /ariel/searches/{search_id} DEPRECATED . . . . .	289

DELETE /ariel/searches/{search_id} DEPRECATED . . . . .	291
GET /ariel/searches/{search_id}/results DEPRECATED . . . . .	292
Asset model endpoints . . . . .	293
GET /asset_model/assets DEPRECATED . . . . .	294
POST /asset_model/assets/{asset_id} DEPRECATED . . . . .	295
GET /asset_model/properties DEPRECATED . . . . .	296
GET /asset_model/saved_searches DEPRECATED . . . . .	297
GET /asset_model/saved_searches/{saved_search_id}/results DEPRECATED . . . . .	299
Authentication endpoints . . . . .	300
POST /auth/logout DEPRECATED . . . . .	300
Help endpoints. . . . .	301
GET /help/capabilities DEPRECATED . . . . .	301
QRadar Vulnerability Manager endpoints . . . . .	303
GET /qvm/assets DEPRECATED . . . . .	303
GET /qvm/filters DEPRECATED . . . . .	304
GET /qvm/network DEPRECATED . . . . .	304
GET /qvm/openservices DEPRECATED . . . . .	305
GET /qvm/savedsearches DEPRECATED . . . . .	306
POST /qvm/tickets/assign DEPRECATED . . . . .	306
GET /qvm/vulninstances DEPRECATED . . . . .	307
GET /qvm/vulns DEPRECATED . . . . .	308
Reference data endpoints . . . . .	308
GET /reference_data/map_of_sets DEPRECATED . . . . .	309
POST /reference_data/map_of_sets DEPRECATED . . . . .	310
GET /reference_data/map_of_sets/{name} DEPRECATED . . . . .	311
POST /reference_data/map_of_sets/{name} DEPRECATED . . . . .	313
DELETE /reference_data/map_of_sets/{name} DEPRECATED . . . . .	314
DELETE /reference_data/map_of_sets/{name}/{key} DEPRECATED . . . . .	315
GET /reference_data/maps DEPRECATED . . . . .	317
POST /reference_data/maps DEPRECATED . . . . .	318
GET /reference_data/maps/{name} DEPRECATED . . . . .	319
POST /reference_data/maps/{name} DEPRECATED . . . . .	321
DELETE /reference_data/maps/{name} DEPRECATED . . . . .	322
DELETE /reference_data/maps/{name}/{key} DEPRECATED . . . . .	323
GET /reference_data/sets DEPRECATED . . . . .	325
POST /reference_data/sets DEPRECATED . . . . .	326
GET /reference_data/sets/{name} DEPRECATED . . . . .	327
POST /reference_data/sets/{name} DEPRECATED . . . . .	328
DELETE /reference_data/sets/{name} DEPRECATED . . . . .	330
DELETE /reference_data/sets/{name}/{value} DEPRECATED . . . . .	331
POST /reference_data/sets/bulk_load/{name} DEPRECATED . . . . .	332
GET /reference_data/tables DEPRECATED . . . . .	333
POST /reference_data/tables DEPRECATED . . . . .	335
GET /reference_data/tables/{name} DEPRECATED . . . . .	336
POST /reference_data/tables/{name} DEPRECATED . . . . .	337
DELETE /reference_data/tables/{name} DEPRECATED . . . . .	339
DELETE /reference_data/tables/{name}/{outer_key}/{inner_key} DEPRECATED . . . . .	340
GET /referencedata/mapOfSets DEPRECATED . . . . .	342
POST /referencedata/mapOfSets DEPRECATED . . . . .	343
GET /referencedata/mapOfSets/{name} DEPRECATED . . . . .	344
POST /referencedata/mapOfSets/{name} DEPRECATED . . . . .	346
DELETE /referencedata/mapOfSets/{name} DEPRECATED . . . . .	347
DELETE /referencedata/mapOfSets/{name}/{key} DEPRECATED . . . . .	349
GET /referencedata/maps DEPRECATED . . . . .	350
POST /referencedata/maps DEPRECATED . . . . .	351
GET /referencedata/maps/{name} DEPRECATED . . . . .	352
POST /referencedata/maps/{name} DEPRECATED . . . . .	353
DELETE /referencedata/maps/{name} DEPRECATED . . . . .	354
DELETE /referencedata/maps/{name}/{key} DEPRECATED . . . . .	356
GET /referencedata/sets DEPRECATED . . . . .	357
POST /referencedata/sets DEPRECATED . . . . .	357

GET /referencedata/sets/{name} DEPRECATED . . . . .	359
POST /referencedata/sets/{name} DEPRECATED . . . . .	360
DELETE /referencedata/sets/{name} DEPRECATED . . . . .	361
DELETE /referencedata/sets/{name}/{value} DEPRECATED . . . . .	362
POST /referencedata/sets/bulkLoad/{name} DEPRECATED . . . . .	363
GET /referencedata/tables DEPRECATED. . . . .	364
POST /referencedata/tables DEPRECATED . . . . .	365
GET /referencedata/tables/{name} DEPRECATED . . . . .	366
POST /referencedata/tables/{name} DEPRECATED . . . . .	368
DELETE /referencedata/tables/{name} DEPRECATED . . . . .	369
DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} DEPRECATED . . . . .	371
Scanner endpoints. . . . .	372
GET /scanner/profiles DEPRECATED . . . . .	372
POST /scanner/profiles/create DEPRECATED . . . . .	372
POST /scanner/profiles/start DEPRECATED. . . . .	373
GET /scanner/scanprofiles DEPRECATED . . . . .	374
POST /scanner/scanprofiles DEPRECATED . . . . .	375
GET /scanner/scanprofiles/{profileid} DEPRECATED. . . . .	376
POST /scanner/scanprofiles/{profileid} DEPRECATED . . . . .	377
DELETE /scanner/scanprofiles/{profileid} DEPRECATED . . . . .	378
POST /scanner/scanprofiles/{profileid}/start DEPRECATED . . . . .	379
SIEM endpoints . . . . .	379
GET /siem/local_destination_addresses DEPRECATED . . . . .	380
GET /siem/local_destination_addresses/{local_destination_address_id} DEPRECATED . . . . .	381
GET /siem/offense_closing_reasons DEPRECATED . . . . .	383
POST /siem/offense_closing_reasons DEPRECATED . . . . .	384
GET /siem/offense_closing_reasons/{closing_reason_id} DEPRECATED . . . . .	385
GET /siem/offenses DEPRECATED . . . . .	386
GET /siem/offenses/{offense_id} DEPRECATED . . . . .	389
POST /siem/offenses/{offense_id} DEPRECATED . . . . .	392
GET /siem/offenses/{offense_id}/notes DEPRECATED . . . . .	396
POST /siem/offenses/{offense_id}/notes DEPRECATED. . . . .	397
GET /siem/offenses/{offense_id}/notes/{note_id} DEPRECATED. . . . .	398
GET /siem/source_addresses DEPRECATED. . . . .	400
GET /siem/source_addresses/{source_address_id} DEPRECATED . . . . .	401
REST API V3.0 References . . . . .	402
Ariel endpoints. . . . .	402
GET /ariel/databases DEPRECATED . . . . .	403
GET /ariel/databases/{database_name} DEPRECATED . . . . .	403
GET /ariel/searches DEPRECATED . . . . .	405
POST /ariel/searches DEPRECATED . . . . .	405
GET /ariel/searches/{search_id} DEPRECATED. . . . .	407
POST /ariel/searches/{search_id} DEPRECATED . . . . .	409
DELETE /ariel/searches/{search_id} DEPRECATED . . . . .	410
GET /ariel/searches/{search_id}/results DEPRECATED . . . . .	412
Asset model endpoints . . . . .	413
GET /asset_model/assets DEPRECATED . . . . .	413
POST /asset_model/assets/{asset_id} DEPRECATED . . . . .	414
GET /asset_model/properties DEPRECATED . . . . .	415
GET /asset_model/saved_searches DEPRECATED . . . . .	416
GET /asset_model/saved_searches/{saved_search_id}/results DEPRECATED. . . . .	418
Authentication endpoints . . . . .	419
POST /auth/logout DEPRECATED . . . . .	420
Help endpoints. . . . .	420
GET /help/capabilities DEPRECATED . . . . .	420
QRadar Vulnerability Manager endpoints . . . . .	422
GET /qvm/assets DEPRECATED . . . . .	422
GET /qvm/filters DEPRECATED . . . . .	423
GET /qvm/network DEPRECATED. . . . .	424
GET /qvm/openservices DEPRECATED . . . . .	424
GET /qvm/savedsearches DEPRECATED. . . . .	425



POST /qvm/tickets/assign DEPRECATED . . . . .	426
GET /qvm/vulninstances DEPRECATED . . . . .	427
GET /qvm/vulns DEPRECATED. . . . .	427
Reference Data endpoints . . . . .	428
GET /reference_data/map_of_sets DEPRECATED . . . . .	428
POST /reference_data/map_of_sets DEPRECATED. . . . .	429
GET /reference_data/map_of_sets/{name} DEPRECATED . . . . .	431
POST /reference_data/map_of_sets/{name} DEPRECATED . . . . .	432
DELETE /reference_data/map_of_sets/{name} DEPRECATED . . . . .	434
DELETE /reference_data/map_of_sets/{name}/{key} DEPRECATED. . . . .	435
GET /reference_data/maps DEPRECATED . . . . .	437
POST /reference_data/maps DEPRECATED . . . . .	438
GET /reference_data/maps/{name} DEPRECATED . . . . .	440
POST /reference_data/maps/{name} DEPRECATED . . . . .	441
DELETE /reference_data/maps/{name} DEPRECATED . . . . .	442
DELETE /reference_data/maps/{name}/{key} DEPRECATED . . . . .	444
GET /reference_data/sets DEPRECATED . . . . .	445
POST /reference_data/sets DEPRECATED . . . . .	446
GET /reference_data/sets/{name} DEPRECATED . . . . .	448
POST /reference_data/sets/{name} DEPRECATED. . . . .	449
DELETE /reference_data/sets/{name} DEPRECATED. . . . .	450
DELETE /reference_data/sets/{name}/{value} DEPRECATED . . . . .	452
POST /reference_data/sets/bulk_load/{name} DEPRECATED . . . . .	453
GET /reference_data/tables DEPRECATED . . . . .	454
GET /reference_data/tables/{name} DEPRECATED . . . . .	455
POST /reference_data/tables/{name} DEPRECATED . . . . .	457
DELETE /reference_data/tables/{name} DEPRECATED . . . . .	458
DELETE /reference_data/tables/{name}/{outer_key}/{inner_key} DEPRECATED . . . . .	460
POST /reference_data/tables DEPRECATED . . . . .	461
GET /referencedata/mapOfSets DEPRECATED . . . . .	463
POST /referencedata/mapOfSets DEPRECATED . . . . .	464
GET /referencedata/mapOfSets/{name} DEPRECATED . . . . .	465
POST /referencedata/mapOfSets/{name} DEPRECATED. . . . .	467
DELETE /referencedata/mapOfSets/{name} DEPRECATED. . . . .	468
DELETE /referencedata/mapOfSets/{name}/{key} DEPRECATED . . . . .	470
GET /referencedata/maps DEPRECATED. . . . .	471
POST /referencedata/maps DEPRECATED . . . . .	472
GET /referencedata/maps/{name} DEPRECATED . . . . .	473
POST /referencedata/maps/{name} DEPRECATED . . . . .	474
DELETE /referencedata/maps/{name} DEPRECATED . . . . .	475
DELETE /referencedata/maps/{name}/{key} DEPRECATED . . . . .	477
GET /referencedata/sets DEPRECATED . . . . .	478
POST /referencedata/sets DEPRECATED . . . . .	478
GET /referencedata/sets/{name} DEPRECATED . . . . .	480
POST /referencedata/sets/{name} DEPRECATED . . . . .	481
DELETE /referencedata/sets/{name} DEPRECATED . . . . .	482
DELETE /referencedata/sets/{name}/{value} DEPRECATED . . . . .	483
POST /referencedata/sets/bulkLoad/{name} DEPRECATED . . . . .	484
GET /referencedata/tables DEPRECATED. . . . .	485
POST /referencedata/tables DEPRECATED . . . . .	486
GET /referencedata/tables/{name} DEPRECATED . . . . .	487
POST /referencedata/tables/{name} DEPRECATED . . . . .	489
DELETE /referencedata/tables/{name} DEPRECATED . . . . .	490
DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} DEPRECATED . . . . .	492
Scanner endpoints . . . . .	493
GET /scanner/profiles DEPRECATED . . . . .	493
POST /scanner/scanprofiles DEPRECATED . . . . .	493
POST /scanner/profiles/create DEPRECATED . . . . .	494
POST /scanner/profiles/start DEPRECATED. . . . .	494
GET /scanner/scanprofiles DEPRECATED . . . . .	495
GET /scanner/scanprofiles/{profileid} DEPRECATED. . . . .	497

POST /scanner/scanprofiles/{profileid} DEPRECATED . . . . .	498
DELETE /scanner/scanprofiles/{profileid} DEPRECATED . . . . .	499
POST /scanner/scanprofiles/{profileid}/start DEPRECATED . . . . .	499
SIEM endpoints . . . . .	500
GET /siem/offense_closing_reasons DEPRECATED . . . . .	500
POST /siem/offense_closing_reasons DEPRECATED . . . . .	502
GET /siem/offense_closing_reasons/{closing_reason_id} DEPRECATED . . . . .	503
GET /siem/offenses DEPRECATED . . . . .	504
GET /siem/offenses/{offense_id} DEPRECATED . . . . .	507
POST /siem/offenses/{offense_id} DEPRECATED . . . . .	510
GET /siem/offenses/{offense_id}/notes DEPRECATED . . . . .	513
POST /siem/offenses/{offense_id}/notes DEPRECATED . . . . .	515
GET /siem/offenses/{offense_id}/notes/{note_id} DEPRECATED . . . . .	516
REST API V2.0 References . . . . .	517
Ariel endpoints. . . . .	517
GET /ariel/databases DEPRECATED . . . . .	517
GET /ariel/databases/{database_name} DEPRECATED . . . . .	518
GET /ariel/searches DEPRECATED . . . . .	519
POST /ariel/searches DEPRECATED . . . . .	520
GET /ariel/searches/{search_id} DEPRECATED . . . . .	522
POST /ariel/searches/{search_id} DEPRECATED . . . . .	523
DELETE /ariel/searches/{search_id} DEPRECATED . . . . .	525
GET /ariel/searches/{search_id}/results DEPRECATED . . . . .	526
Asset Model endpoints . . . . .	528
GET /asset_model/assets DEPRECATED . . . . .	528
POST /asset_model/assets/{asset_id} DEPRECATED . . . . .	529
GET /asset_model/properties DEPRECATED . . . . .	530
GET /asset_model/saved_searches DEPRECATED . . . . .	531
GET /asset_model/saved_searches/{saved_search_id}/results DEPRECATED . . . . .	533
Authentication endpoints . . . . .	534
POST /auth/logout DEPRECATED . . . . .	534
Help endpoints. . . . .	535
GET /help/capabilities DEPRECATED . . . . .	535
QRadar Vulnerability Manager endpoints . . . . .	537
GET /qvm/assets DEPRECATED . . . . .	537
GET /qvm/filters DEPRECATED . . . . .	538
GET /qvm/network DEPRECATED . . . . .	539
GET /qvm/openservices DEPRECATED . . . . .	539
GET /qvm/savedsearches DEPRECATED . . . . .	540
POST /qvm/tickets/assign DEPRECATED . . . . .	541
GET /qvm/vulninstances DEPRECATED . . . . .	541
GET /qvm/vulns DEPRECATED . . . . .	542
Reference Data endpoints . . . . .	543
GET /reference_data/map_of_sets DEPRECATED . . . . .	543
POST /reference_data/map_of_sets DEPRECATED . . . . .	544
GET /reference_data/map_of_sets/{name} DEPRECATED . . . . .	546
POST /reference_data/map_of_sets/{name} DEPRECATED . . . . .	547
DELETE /reference_data/map_of_sets/{name} DEPRECATED . . . . .	548
DELETE /reference_data/map_of_sets/{name}/{key} DEPRECATED . . . . .	550
GET /reference_data/maps DEPRECATED . . . . .	551
POST /reference_data/maps DEPRECATED . . . . .	552
GET /reference_data/maps/{name} DEPRECATED . . . . .	554
POST /reference_data/maps/{name} DEPRECATED . . . . .	555
DELETE /reference_data/maps/{name} DEPRECATED . . . . .	557
DELETE /reference_data/maps/{name}/{key} DEPRECATED . . . . .	558
GET /reference_data/sets DEPRECATED . . . . .	559
POST /reference_data/sets DEPRECATED . . . . .	561
GET /reference_data/sets/{name} DEPRECATED . . . . .	562
POST /reference_data/sets/{name} DEPRECATED . . . . .	563
DELETE /reference_data/sets/{name} DEPRECATED . . . . .	565
DELETE /reference_data/sets/{name}/{value} DEPRECATED . . . . .	566

POST /reference_data/sets/bulk_load/{name} DEPRECATED . . . . .	567
GET /reference_data/tables DEPRECATED . . . . .	568
POST /reference_data/tables DEPRECATED . . . . .	570
GET /reference_data/tables/{name} DEPRECATED . . . . .	571
POST /reference_data/tables/{name} DEPRECATED . . . . .	573
DELETE /reference_data/tables/{name} DEPRECATED . . . . .	574
DELETE /reference_data/tables/{name}/{outer_key}/{inner_key} DEPRECATED . . . . .	576
GET /referencedata/mapOfSets DEPRECATED . . . . .	577
POST /referencedata/mapOfSets DEPRECATED . . . . .	578
GET /referencedata/mapOfSets/{name} DEPRECATED . . . . .	579
POST /referencedata/mapOfSets/{name} DEPRECATED . . . . .	581
DELETE /referencedata/mapOfSets/{name} DEPRECATED . . . . .	583
DELETE /referencedata/mapOfSets/{name}/{key} DEPRECATED . . . . .	584
GET /referencedata/maps DEPRECATED . . . . .	585
POST /referencedata/maps DEPRECATED . . . . .	586
GET /referencedata/maps/{name} DEPRECATED . . . . .	587
POST /referencedata/maps/{name} DEPRECATED . . . . .	588
DELETE /referencedata/maps/{name} DEPRECATED . . . . .	590
DELETE /referencedata/maps/{name}/{key} DEPRECATED . . . . .	591
GET /referencedata/sets DEPRECATED . . . . .	592
POST /referencedata/sets DEPRECATED . . . . .	592
GET /referencedata/sets/{name} DEPRECATED . . . . .	594
POST /referencedata/sets/{name} DEPRECATED . . . . .	595
DELETE /referencedata/sets/{name} DEPRECATED . . . . .	596
DELETE /referencedata/sets/{name}/{value} DEPRECATED . . . . .	597
POST /referencedata/sets/bulkLoad/{name} DEPRECATED . . . . .	598
GET /referencedata/tables DEPRECATED . . . . .	599
POST /referencedata/tables DEPRECATED . . . . .	600
GET /referencedata/tables/{name} DEPRECATED . . . . .	602
POST /referencedata/tables/{name} DEPRECATED . . . . .	603
DELETE /referencedata/tables/{name} DEPRECATED . . . . .	605
DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} DEPRECATED . . . . .	606
Scanner endpoints . . . . .	607
GET /scanner/profiles DEPRECATED . . . . .	607
POST /scanner/profiles/create DEPRECATED . . . . .	608
POST /scanner/profiles/start DEPRECATED . . . . .	608
GET /scanner/scanprofiles DEPRECATED . . . . .	609
POST /scanner/scanprofiles DEPRECATED . . . . .	611
GET /scanner/scanprofiles/{profileid} DEPRECATED . . . . .	611
POST /scanner/scanprofiles/{profileid} DEPRECATED . . . . .	613
DELETE /scanner/scanprofiles/{profileid} DEPRECATED . . . . .	614
POST /scanner/scanprofiles/{profileid}/start DEPRECATED . . . . .	614
Offense endpoints . . . . .	615
GET /siem/offenses DEPRECATED . . . . .	615
<b>Notices . . . . .</b>	<b>619</b>
Privacy policy considerations . . . . .	620



---

## About this guide

The IBM® Security QRadar® API Reference Guide provides information on the RESTful API for how to integrate QRadar solutions into third-party systems.

### Intended audience

This guide is intended for developers with coding experience. This guide assumes that you have QRadar access and a knowledge of your corporate network and networking technologies.

### Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

### Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

### Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

#### Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.



---


## Chapter 1. What's new for developers in RESTful APIs in QRadar V7.2.6

IBM Security QRadar V7.2.6 introduces version 5.0 of the API endpoints.

### New endpoints

QRadarV7.2.6 introduces several new endpoints:


- GUI application framework API endpoints
- Tenant management API endpoints
- Domain management API endpoints
- Extension management API endpoints
- Custom action API endpoints
- Security posture API endpoints

 [Learn More...](#)

### Deprecated endpoints


All version 2.0, 3.0, and 3.1 API endpoints are marked as deprecated in QRadar V7.2.6.

All version 0.1, 0.2, and 1.0 API endpoints are removed in QRadar V7.2.6.

 [Learn More...](#)

### Filter criteria

You can now apply filters on fields stored inside an array using the new CONTAINS and LIKE operators.

 [Learn More...](#)

### Reference Data GET endpoints access

With the new read-only permissions to reference data you can now access all versions of the reference data GET endpoints. Previously, you were required to have Admin privileges.

---

## New endpoints in more detail

V7.2.6 of IBM Security QRadar significantly expands the number of endpoints that are available in the QRadar API. New areas of QRadar functionality are opened with the following new endpoints.

### GUI Application Framework endpoints

GUI Application Framework endpoints:

Use these endpoints to install and manage applications that you create by using the GUI Application Framework Software Development Kit.

- 5.0 GET /gui\_app\_framework/application\_creation\_task  
Retrieves a list of status details of all asynchronous requests to create apps.
- 5.0 POST /gui\_app\_framework/application\_creation\_task  
Creates an app within the app framework, and registers it with QRadar.
- 5.0 GET /gui\_app\_framework/application\_creation\_task/{application\_id}  
Retrieves the status details for an asynchronous request that is used to create an app.
- 5.0 POST /gui\_app\_framework/application\_creation\_task/{application\_id}  
Updates a new app that is installed within the app framework.
- 5.0 GET /gui\_app\_framework/applications  
Retrieves a list of apps that are installed on the QRadar console.
- 5.0 GET /gui\_app\_framework/applications/{application\_id}  
Retrieves a specific app that is installed on the QRadar console.
- 5.0 POST /gui\_app\_framework/applications/{application\_id}  
Updates an app. Starts or stops an app by setting status to RUNNING or STOPPED respectively.
- 5.0 DELETE /gui\_app\_framework/applications/{application\_id}  
Deletes an app.

## Tenant management API endpoints

Use these endpoints to manage tenants in multitenancy environments.

- 5.0 GET /config/access/tenant\_management/tenants  
Retrieves an ordered list of tenants by tenant ID.
- 5.0 POST /config/access/tenant\_management/tenants  
Creates a tenant.
- 5.0 GET /config/access/tenant\_management/tenants/{tenant\_id}  
Retrieves a tenant by tenant ID.
- 5.0 POST /config/access/tenant\_management/tenants/{tenant\_id}  
Updates a tenant.
- 5.0 DELETE /config/access/tenant\_management/tenants/{tenant\_id}  
Deletes a tenant.

## Domain management API endpoints

Use these endpoints to create and manage domains in multidomain environments.

- 5.0 GET /config/domain\_management/domains  
Retrieves the list of all domain objects, including objects in active and deleted domains, including the default domain.
- 5.0 POST /config/domain\_management/domains  
Creates a domain.
- 5.0 GET /config/domain\_management/domains/{domain\_id}  
Retrieves a domain resource by the domain ID.
- 5.0 POST /config/domain\_management/domains/{domain\_id}  
Updates an existing domain.



- 5.0 DELETE /config/domain\_management/domains/{domain\_id}  
Deletes a domain by domain ID. All domain mappings are also deleted.

## Extension management API endpoints

Use these endpoints to install, uninstall, and manage QRadar extensions.

- 5.0 GET /config/extension\_management/extensions  
Retrieves a list of extensions.
- 5.0 POST /config/extension\_management/extensions  
Uploads the extension file to the QRadar system.
- 5.0 GET /config/extension\_management/extensions/{extension\_id}  
Retrieves an extension based on the supplied extension ID.
- 5.0 POST /config/extension\_management/extensions/{extension\_id}  
Install the specified extension.
- 5.0 DELETE /config/extension\_management/extensions/{extension\_id}  
Uninstall the specified extension.
- 5.0 GET /config/extension\_management/extensions\_task\_status/{status\_id}  
Retrieves the specified task's status.
- 5.0 GET /config/extension\_management/extensions\_task\_status/{status\_id}/results  
Retrieves the the specified task's status.

## Custom action API endpoints

Use these endpoints to create, update, and remove custom actions and custom action scripts that are used in the custom rule engine (CRE).

- 5.0 GET /analytics/custom\_actions/actions  
Retrieves a list of available custom actions.
- 5.0 POST /analytics/custom\_actions/actions  
Creates a custom action.
- 5.0 GET /analytics/custom\_actions/actions/{action\_id}  
Retrieves the specified custom action.
- 5.0 POST /analytics/custom\_actions/actions/{action\_id}  
Updates an existing custom action.
- 5.0 DELETE /analytics/custom\_actions/actions/{action\_id}  
Deletes an existing custom action.
- 5.0 GET /analytics/custom\_actions/interpreters  
Retrieves a list of available custom action interpreters.
- 5.0 GET /analytics/custom\_actions/interpreters/{interpreter\_id}  
Retrieves the specified custom action interpreter.
- 5.0 GET /analytics/custom\_actions/scripts  
Retrieves a list of metadata for the custom action script that are available.
- 5.0 POST /analytics/custom\_actions/scripts  
Creates a custom action script.
- 5.0 GET /analytics/custom\_actions/scripts/{script\_id}  
Retrieves metadata for the specified custom action script file.
- 5.0 POST /analytics/custom\_actions/scripts/{script\_id}

Updates an existing custom action script.

- 5.0 DELETE /analytics/custom\_actions/scripts/{script\_id}  
Deletes an existing custom action script.

## Security posture API endpoints

Use these endpoints to manage server hosts, network interfaces and firewall rules.

- 5.0 GET /system/servers  
Retrieves a list of all servers in the deployment.
- 5.0 GET /system/servers/{server\_id}  
Retrieves the specified server.
- 5.0 POST /system/servers/{server\_id}  
Updates an existing server.
- 5.0 GET /system/servers/{server\_id}/network\_interfaces/bonded  
Retrieves a list of the bonded network interfaces for the specified server.
- 5.0 POST /system/servers/{server\_id}/network\_interfaces/bonded/{device\_name}  
Updates an existing bonded network interface for the specified server.
- 5.0 GET /system/servers/{server\_id}/network\_interfaces/ethernet  
Retrieves a list of the Ethernet network interfaces for the specified server.
- 5.0 POST /system/servers/{server\_id}/network\_interfaces/ethernet/{device\_name}  
Updates an Ethernet network interface for the specified server ID and device name.
- 5.0 PUT /system/servers/{server\_id}/firewall\_rules  
Replaces the access control firewall rules for the specified server with the firewall rules that are in the request.
- 5.0 GET /system/servers/{server\_id}/firewall\_rules  
Retrieves a list of access control firewall rules for the specified server.

---

## Deprecated endpoints in more detail

All version 2.0, 3.0, and 3.1 API endpoints are marked as deprecated in IBM Security QRadar V7.2.6.

Although deprecated endpoints continue to function, they will be removed in a future release. You must update your integration to use version 5.0, the latest version of the API. Responses to deprecated endpoint requests include a Deprecated response header that indicates that the endpoint is deprecated.

All version 0.1, 0.2, and 1.0 API endpoints are removed in QRadar V7.2.6.

### Related concepts:

Chapter 2, “RESTful API overview,” on page 5

You access the RESTful API by sending HTTPS requests to specific URLs (endpoints) on the QRadar Console. To send these requests, use the HTTP implementation that is built in to the programming language of your choice. Each request contains authentication information, and parameters that modify the request.

---

## Chapter 2. RESTful API overview

You access the RESTful API by sending HTTPS requests to specific URLs (endpoints) on the QRadar Console. To send these requests, use the HTTP implementation that is built in to the programming language of your choice. Each request contains authentication information, and parameters that modify the request.

### API Endpoints

An API *endpoint* contains the URL of the resource that you want to access and the action that you want to complete on that resource. The action is indicated by the HTTP method of the request: GET, POST, PUT, or DELETE.

### Required permissions to access the API

Authentication information must be included in every API request as an HTTP header. Provide the required access credentials in one of the following ways:

- A user name and password for a QRadar user that is specified in the authorization header.

You specify the user name and password by using HTTP basic authentication. Although you can make API requests by providing a user name and password for every request, use authorized service tokens for all API integrations with QRadar. Only the user name and password option is supported for viewing the Documentation Page.

For more information about creating user roles, security profiles, and users, see the *IBM Security QRadar SIEM Administration Guide*.

- An authorized services token that is specified in the SEC header.

To authenticate as an authorized service, you create an authentication token that uses authorized services. QRadar authorized services have roles and security profiles assigned that control access to the various API resources.

The token is valid until the expiry date that you specified when you created the authorized service.

For more information about creating user roles, security profiles and authorized services, see the *IBM Security QRadar SIEM Administration Guide*.

The following table highlights the required role and the security profile impacts for each API endpoint:

*Table 1. Role permissions and security profile requirements*

API Endpoints	Roles Permissions	Security Profile
/api/analytics/*	Requires <b>Admin</b> permission.	Requires Admin security profile.
/api/ariel/*	Requires <b>Admin</b> permission for querying events or flows.	Requires Admin security profile.
/api/asset_model/*	Requires <b>Vulnerability Management</b> or <b>Assets</b> permissions.	Data returned restricted based on security profile assigned.
/api/auth/*	No permission restrictions.	No security profile restrictions.

Table 1. Role permissions and security profile requirements (continued)

API Endpoints	Roles Permissions	Security Profile
/api/config/access/tenant_management	Requires <b>Admin</b> permission.	Requires Admin security profile.
/api/config/domain_management	Requires <b>Admin</b> permission.	Requires Admin security profile.
/api/config/extensions_management	Requires <b>Admin</b> permission.	Requires Admin security profile.
/api/gui_app_framework/*	Requires <b>Admin</b> permission.	Requires Admin security profile.
/api/help/*	No permission restrictions.	No security profile restrictions.
/api/qvm/*	Requires <b>Assets</b> permissions.	Requires a security profile with access to all networks, all log sources, and all domains.
/api/reference_data/*	Requires <b>Admin</b> permissions for POST and DELETE requests. Requires <b>View Reference Data</b> for GET requests.	Requires Admin security profile.
/api/scanner/*	Requires <b>Vulnerability Management</b> permissions.	Requires a security profile with access to all networks, all log sources, and all domains.
/api/siem/*	Requires <b>Offenses</b> permissions.  The <b>Manage Offense Closing Reasons</b> permission is required for creating offense closing reasons ( <b>POST /api/siem/offense_closing_reasons</b> ). The <b>Assign Offenses to Users</b> permission is required for updating the assigned to field of an offense ( <b>POST /api/siem/offenses/{offense_id}</b> when the <b>assigned_to</b> parameter is supplied).	Data returned restricted based on security profile assigned.
/api/system/*	Requires <b>Admin</b> permission.	Requires Admin security profile.

## API requests and responses

When you send an API request, the server returns an HTTP response. The HTTP response contains a status code to indicate whether the request succeeded and the details of the response in the response body. Most resources format this response as JavaScript Object Notation (JSON). You can use the JSON packages or libraries that are built in to the programming language that you use to extract the data.

For a complete example of this process, see the sample code in GitHub (<https://github.com/ibm-security-intelligence/api-samples>).

## Version headers

You use version headers to request a specific version of the API. If you don't provide a version header, the latest version of the API is used, which might break integrations when QRadar is upgraded. If you provide a version header every time you use an API, it makes it easier to upgrade to newer versions of QRadar without breaking your API clients.

The APIs use the major and minor components of semantic versioning. Natural numbers are used to designate major versions of the API, for example, '3'. Minor versions of the API are designated with a major and minor component, for example, '3.1'. You can set the version header to a major or a minor version of the API. Changes that are compatible with existing versions are introduced with an incremented minor version number. Any incompatible changes are introduced with a major version number increment.

When a major version of the API is specified in the version header without a minor component, the server responds with the latest minor version within the major API version. For example, if the client requests version '3', the server responds with version '3.1'. If you want to use version 3.0, you must request '3.0' in the version header. If you request a version greater than the latest version of an endpoint, the latest available version of that endpoint is returned. Each endpoint is listed under every version it is valid for, even if it's unchanged in the newer versions.

## Endpoint deprecation

An API endpoint is marked as *deprecated* to indicate that it is not recommended for use and will be removed in a future release. To give integrations time to use an alternative, a deprecated endpoint continues to function for at least 1 release before it is removed. The interactive API documentation page indicates that an endpoint is marked as deprecated. Also, the API response message for a deprecated endpoint includes the header `Deprecated`. An individual API endpoint, or an entire version of API endpoints can be marked as deprecated. The deprecated endpoints still continue to function until they are removed.

When an API endpoint completes the deprecation process, it is removed. Endpoints that are removed no longer respond successfully. An attempt to call a removed endpoint returns an error. An HTTP 410 Gone response is returned for individual removed endpoints. An HTTP 422 Unprocessable Entity response is returned for requests for a version that is no longer supported.

Include the version header in API requests to call a specific version of an API endpoint. API integrations that do not explicitly request a particular version are not supported. If you do not specify a version, your request is directed to the latest available version. If a release includes a new, incompatible version of an endpoint, your integration might break. Have your request version in one location in your code to ease upgrading as newer versions become available.

## Filter syntax

To limit the results that are returned in an API retrieval request (HTTP GET), most IBM Security QRadar API endpoints that return lists of resources support the **filter** parameter.

The **filter** parameter syntax is consistent for all endpoints that support it. Refer to the documentation for the endpoint to determine if the filter parameter applies to it. Any limitations for the filter syntax are included in that endpoint's description. You are reminded that query parameters must be double URL encoded before they are sent.

### Comparison Operators

The filter comparison operators table describes the comparison operators that you can use as part of the filter parameter.

Table 2. Filter comparison operators

Operator	Description	Example Filter Syntax
=	Equality between the identifier and the specified value returned.	To find offenses where <i>status</i> =CLOSED: GET /api/siem/offenses?filter=status%3DCLOSED
>	Identifier is greater than the specified value.	To find offenses where <i>credibility</i> > 3: /api/siem/offenses?filter=credibility%20%3E%203
<	Identifier is less than the specified value.	To find offenses where <i>magnitude</i> < 9: /api/siem/offenses?filter=magnitude%20%3C%209
<=	Identifier is less than or equal to the specified value.	To find offenses where <i>id</i> <= 1004: /api/asset_model/properties?filter=id%20%3C%3D%201004
>=	Identifier is greater than or equal to the specified value.	To find offenses where <i>scanProfileId</i> >= 3: /api/scanner/ scanprofiles?filter=scanProfileId%20%3E%3D%203
!=, <>, ^=	Identifier is not equal to the specified value.	The following examples filters all IDs that are not equal to 5: /api/siem/offenses?filter=id%20!%3D%205  /api/siem/offenses?filter=id%20%3C%3E%205  /api/siem/offenses?filter=id%20%5E%3D%205
in	Identifier is equal to at least one of the specified values in the list.	<i>id</i> in (1001,1111,1200): /api/asset_model/assets?filter=id%20in%20(1001%2C1111%2C1200)

Table 2. Filter comparison operators (continued)

Operator	Description	Example Filter Syntax
not in	Identifier is not equal to any of the specified values in the list.	<code>id not in (1001,1002,1003):</code>  <code>/api/asset_model/saved_searches?filter=id%20not%20in%20(14%2C20%2C1003)</code>
between ... and ...	Identifier is between 2 specified values.	<code>id between 0 and 3:</code>  <code>/api/siem/offenses?filter=id%20between%200%20and%203</code>
not between ... and ...	Identifier is not between 2 specified values.	<code>id not between 30 and 31:</code>  <code>/api/siem/offenses?filter=id%20not%20between%2030%20and%2031</code>
is null	Identifier is null.	<code>assigned_to is null:</code>  <code>/api/siem/offenses?filter=assigned_to%20is%20null</code>
is not null	Identifier is not null.	<code>assigned_to is not null:</code>  <code>/api/siem/offenses?filter=assigned_to%20is%20not%20null</code>

## Null values and comparison operators

When the field that you filtered on has a 'null' value, comparison operators behave in the following ways:

- "=", ">", ">=", "<", "<=", "IN", and "BETWEEN" operators always return false
- "!=", "<>", "^=", "NOT BETWEEN", and "NOT IN" always return true

The best way to test for null values is to use the "is null" or "is not null" operators.

## Logical operators

Use the logical operators **OR**, **AND**, and **NOT** to perform logical operations on subexpressions. The following table provides examples of how to use logical operators in filters.

Operator	Description	Example
or	Performs a logical <b>OR</b> operation on the 2 subexpressions. The subexpressions might be comparison nodes or other logical nodes.	<code>assigned_to is not null OR id = 111:</code>  <code>/api/siem/offenses?filter=assigned_to%20is%20not%20null%20or%20id%20%3D%20111</code>
and	Performs a logical <b>AND</b> operation on the 2 sub-expressions. The sub-expressions might be comparison nodes or other logical nodes.	<code>assigned_to is not null AND id = 111:</code>  <code>/api/siem/offenses?filter=assigned_to%20is%20not%20null%20and%20id%20%3D%20111</code>

Operator	Description	Example
not	Performs a logical <b>NOT</b> operation on the subexpression.	<code>protected =true and not id in (111,112,113)</code>  <code>/api/siem/offenses?filter=protected%20%3D%20true%20and%20not%20id%20in%20(111%2C112%2C113)</code>

## Specifying JSON fields for comparisons

The following table explains how to specify JSON fields for use with comparison operators in filters.

JSON field example	Description	Example
<pre>{   "name": "Proprietary Data",   "element_type": "ALN" }</pre>	When you apply a filter to a field directly in the object that is returned, the field is specified by name.	<code>name = "Proprietary Data"</code>  <code>GET /api/reference_data/sets?filter=name%20%3D%20%22Proprietary%20Data%22</code>
<pre>{   "description": "String",   "duration": {     "days": 42,     "hours": 42,     "minutes": 42,     "months": 42,     "seconds": 42.5,     "years": 42   } }</pre>	When you apply a filter to a field nested inside a sub object use brackets to specify the inner field.	<code>duration(days) &gt;= 20</code>  <code>GET /api/scanner/scanprofiles?filter=duration(days)%20%3E%3D%201</code>
<code>["events","flows","simarc"]</code>	For simple JSON types where there is no field label, such as strings, numbers or Boolean, use the <code>.</code> operator.	<code>.= events</code>  <code>GET /api/ariel/databases?filter=%3D%20events</code>

## Specifying string and numeric values in filters

When you filter on string that have values with non-alphanumeric characters, you must wrap the target string in quotation marks. When you filter on numeric values, the numeric values can follow these conditions:

- Start with a leading + or - sign.
- Contain or start with a decimal point
- Include an exponent using e notation.

## Filtering complex objects by using the CONTAINS operator

You filter complex objects by using the CONTAINS operator. You use the CONTAINS operator to test the contents of lists or maps. On the left side of the operator, is an identifier that is in the standard format, for example `x(y(z))`. The identifier must refer to an element that is a list, map, or collection. On the right



side, of the operator is an expression that specifies how the objects in the list must be matched. There are two basic uses for the CONTAINS operator:

- The list that is examined contains simple elements like strings or numbers
- The list contains complex objects.

#### **Lists that contain simple types**

For lists that contain simple types such as strings or numbers, the expression is a value of the same type. For single comparisons, no brackets are required

To request only asset saved searches that have *ftp* as the string in the filter's value field:

```
GET /api/asset_model/saved_searches?filter=filters%20contains%20value%20%3D%20ftp
```

To request assets where interfaces contains the IP address "1.2.3.4":

```
GET /api/asset_model/assets?filter=interfaces%20contains%20ip_addresses%20contains%20value%20%3D%20%221.2.3.4%22
```

#### **Lists that contain complex objects**

For lists that contain complex objects, the expression is a complete filter expression for the objects within the list. This subfilter expression uses the same syntax as any other filter. You can use any operator in the subfilter to test sublists inside the original list. Identifiers in this expression are relative to the objects in the list that the CONTAINS operator is operating on. In complex subfilter expressions, brackets are required.

To request only assets that have a field value = 14 and the Greater than operator , apply the filter filters contains (value = 14 or operator = "Greater than"). This filter returns the first and the last elements in the list.

```
GET /api/asset_model/saved_searches?filter=filters%20contains%20(value%20%3D%2014%20and%20operator%20%3D%20%22Greater%20than%22)
```

To find offenses that contain source addresses that have ID values less than 3 apply the following filter:

```
GET /api/siem/offenses?filter=source_address_ids%20contains%20(.%20%3C3)
```

## **The LIKE operator**

Use the LIKE operator to retrieve partial string matches.

The LIKE operator uses the following format: identifier like "expression". Quotation marks around the expression is mandatory. Single and double quotation marks are supported. The LIKE keyword does case-sensitive matching.

The following wildcard characters are supported. If you use wildcard characters in a string, you must use escape them.

Wildcard character	Description
%	Matches a string of zero or more characters
_	Matches any single character

You can combine the wildcards in the same expression. For example, to find the reference set whose name ends with *Data* and begins with *H*:

```
GET /api/reference_data/sets?filter=name%20like%20%22H_%25Data%22
```

---

## Sort syntax

To order the results that are returned in an API retrieval request, HTTP GET, some IBM Security QRadar API endpoints that return lists of resources support the **sort** parameter.

The **sort** parameter syntax is consistent for all endpoints that support it. Refer to the documentation for the endpoint to determine if the sort parameter applies to it. Any limitations on the sort syntax are included in that endpoint's description. To ensure that spaces or special characters are encoded properly, remember that query parameters must be double URL encoded before they are sent.

### Sort operators

Operator	Description	Example
+	Sort field is in ascending order.	Sort <i>add_time</i> field in ascending order:  <code>/api/config/extension_management/extensions?sort=%2Badd_time</code>
-	Sort field is in descending order.	Sort <i>version</i> field in descending order:  <code>/api/config/extension_management/extensions?sort=-version</code>

### Sorting multiple fields

You can sort multiple fields by separating them with a comma. In the following example, the *version* field is sorted in descending order. Then, within each version group, the *add\_time* field is sorted in ascending order.

```
/api/config/extension_management/extensions?sort=-version%2C%2Badd_time
```

### Escaping characters in sort strings

Escape any character in the sort string by preceding it with a backslash (\). If any of the following characters are inside a field identifier, you must escape them:

- ,
- (
- )
- \

---

## Paging syntax

To limit the results returned in an API retrieval request, HTTP GET, most IBM Security QRadar API endpoints that return lists of resources support the **Range** header parameter.

The **Range** parameter syntax is consistent for all endpoints that support it. Refer to the documentation for the endpoint to determine whether the **Range** parameter applies to it. Any limitations on the **Range** syntax are included in that endpoint's description.

**Note:** The **Range** parameter is always sent as a header parameter, unlike the **sort**, **filter**, and **fields** parameters. These parameters are typically query parameters.

By default, only the first 50 records are returned for the **Range** parameter on the interactive API documentation page. You can alter the **Range** value for an endpoint. However, if you request large result sets, it might negatively affect the performance of the interactive API documentation page.

## Range header parameter

Paging requests are specified with the **Range** header parameter. Use the following zero-indexed syntax:

```
Range: items=x-y
```

The response to a request that employs paging includes the Content-Range header. The header indicates the number of records that were returned within the content range in the following format:

```
Content-Range: items x-y/total number of records received
```

For example, to return the first 5 records, the request header contains the following parameter:

```
"Range: items= 0-4"
```

The response header for that request returns the following information:

```
Content-Range: items 0-4/5
```

If the requested range exceeds the number of records, all records that are within the stated range are returned. In the following example, the first 100 records are requested:

```
"Range: items= 0-99"
```

However, there are only 12 records in total. The response returns all records within the stated range:

```
Content-Range: items 0-11/12
```

If the range requested is beyond the bounds of the amount of records, then no records are returned. In the following example, the first records 3 to 5 records are requested:

```
"Range: items = 3-5"
```

However, there are fewer than 3 records, and so no records are returned:

```
Content-Range: items */3
```

---

## API error messages

When an API request fails due to request errors or server errors, an error response message is returned in JSON format.

An error response message is returned in JSON format even for endpoints that support other MIME types. The error response message includes error message itself, a description of the error, a unique error code for the endpoint, an HTTP response message, and an HTTP response code.

The error response includes following fields:

- **message**: the error message
- **details**: a field for additional information, which may or may not be populated
- **description**: description of the specific error

- **code:** Unique error response code
- **http\_response:**
  - **message:** HTTP response message
  - **code:** HTTP response status code

For example, the following API request attempts to get information about a non-existent reference set that is called “test-set”

https://<host\_ip>/api/reference\_data/sets/test\_set

An HTTP 404 response code and the following JSON error response message are returned:

```
{
  "message": "test_set does not exist",
  "details": {},
  "description": "The reference set does not exist.",
  "code": 1002,
  "http_response": {
    "message": "We could not find the resource you requested.",
    "code": 404
  }
}
```

The following table provides more information about the HTTP response error categories returned by the IBM Security QRadar REST API:

HTTP error category	HTTP response Code	HTTP response message
MULTIPLE CHOICES	300	The requested resource corresponds to any one of a set of representations, each with its own specific location.
MOVED PERMANENTLY	301	The resource has moved permanently. Please refer to the documentation.
FOUND	302	The resource has moved temporarily. Please refer to the documentation.
SEE OTHER	303	The resource can be found under a different URI.
NOT MODIFIED	304	The resource is available and not modified.
USE PROXY	305	The requested resource must be accessed through the proxy given by the Location field.
TEMPORARY REDIRECT	307	The resource resides temporarily under a different URI.
BAD REQUEST	400	Invalid syntax for this request was provided.
UNAUTHORIZED	401	You are unauthorized to access the requested resource. Please log in.
FORBIDDEN	403	Your account is not authorized to access the requested resource.
NOT FOUND	404	We could not find the resource you requested. Please refer to the documentation for the list of resources.

<b>HTTP error category</b>	<b>HTTP response Code</b>	<b>HTTP response message</b>
METHOD NOT ALLOWED	405	This method type is not currently supported.
NOT ACCEPTABLE	406	Acceptance header is invalid for this endpoint resource.
PROXY AUTHENTICATION REQUIRED	407	Authentication with proxy is required.
REQUEST TIMEOUT	408	Client did not produce a request within the time that the server was prepared to wait.
CONFLICT	409	The request could not be completed due to a conflict with the current state of the resource.
GONE	410	The requested resource is no longer available and has been permanently removed.
LENGTH REQUIRED	411	Length of the content is required, please include it with the request.
PRECONDITION FAILED	412	The request did not match the pre-conditions of the requested resource.
REQUEST ENTITY TOO LARGE	413	The request entity is larger than the server is willing or able to process.
REQUEST-URI TOO LONG	414	The request URI is longer than the server is willing to interpret.
UNSUPPORTED MEDIA TYPE	415	The requested resource does not support the media type provided.
REQUESTED RANGE NOT SATISFIABLE	416	The requested range for the resource is not available.
EXPECTATION FAILED	417	Unable to meet the expectation given in the Expect request header.
MISSING ARGUMENTS	419	The requested resource is missing required arguments.
INVALID ARGUMENTS	420	The requested resource does not support one or more of the given parameters.
UNPROCESSABLE ENTITY	422	The request was well-formed but was unable to be followed due to semantic errors.
INTERNAL SERVER ERROR	500	Unexpected internal server error.
NOT IMPLEMENTED	501	The requested resource is recognized but not implemented.
BAD GATEWAY	502	Invalid response received when acting as a proxy or gateway.
SERVICE UNAVAILABLE	503	The server is currently unavailable.
GATEWAY TIMEOUT	504	Did not receive a timely response from upstream server while acting as a gateway or proxy.

HTTP error category	HTTP response Code	HTTP response message
HTTP VERSION NOT SUPPORTED	505	The HTTP protocol version used in the request message is not supported.
INITIALIZATION FAILURE	550	A failure occurred during initialization of services. API will be unavailable.

---

## Cross-origin resource sharing

Cross-origin resource sharing (CORS) occurs when a script on one server sends an Ajax request to another server. Cross-origin resource sharing also occurs when a request is sent on a different protocol or port to the same server.

Cross-origin resource sharing violates the 'same origin policy', which is in place to prevent cross-site request forgery attacks. While the global prevention of cookies for `/api/*` endpoints avoids these attacks, browsers still attempt to enforce this policy. All browsers use this convention but it does not apply to manual request mechanisms like `cURL`.

Browsers detect that you are attempting to make a request to a server, and initially send a preflight request. Preflight requests are set as an `OPTION` request against the same URL, but also contain the `Origin` header. The server must send back other information such as allowed request types, whether to expect headers in the actual request's response, and whether the origin is accepted.

If the `'Access-Control-Allow-Origin'` header of the response of the preflight request does not match the `Origin` header of the request, the browser rejects it. If the `'Access-Control-Allow-Origin'` header matches, the browser proceeds with the request. The request's response must pass the same origin check, in case the rule changes between the preflight and actual request.

### Management of allowed origins

The origin value that is sent by your browser contains the protocol followed by the host name and port, for example:

```
http://1.2.3.4:8888
```

You can intercept requests sent by your browser to ensure that you have the correct origin value. You can add your origin to a whitelist on the QRadar Console in the `/opt/qradar/webapps/console/restapi/allowed_origins.list` file. Changes are detected and take effect immediately. This file contains a newline separated list of allowed origins. Each entry is tested against the origin header that is sent by browsers during pre-flight requests. If an entry matches the origin (or any entry is `*`), the browser is allowed to make cross-origin resource sharing requests.

A common browser convention is to send `null` as the origin when the script is started from `file://` by adding `*` to the whitelist. This practice allows all origins and is not a good practice.

---

## Chapter 3. API command-line client

Use the API command-line client to make API calls when logged in to the IBM Security QRadar host as the root user. The API command-line client is experimental and will stabilize over future QRadar releases.

You can use the API command-line client to complete the following tasks:

1. Print API endpoints. To print all endpoints and information that is required to make calls against the endpoints, use the following command:

```
/opt/qradar/bin/api_client --print_api
```

2. Make requests to API endpoints.

### Basic API calls

A basic API call is a GET request to an endpoint that requires no parameters, for example:

```
/opt/qradar/bin/api_client --api /help/capabilities --method GET
```

The following table provides the arguments that you can use for basic calls.

Table 3. Arguments for basic calls

Argument	Definition
--api /api_name/endpoint	The path to your API endpoint. This path appends to <code>https://ConsoleIPaddress/</code> . For example: <code>https://ConsoleIPaddress/api/reference_data/sets/</code>
--method METHOD	Determines whether your API request is a GET, POST, or DELETE method. View the output of <code>--print_api</code> for the required method.

### Calls with path parameters

You can add path parameters to modify the endpoint that you want to call and correspond to a place in the endpoint portion in the URL. Use the **Name** parameter, for example:

```
/referencedata/sets/{name}
```

To call a specific reference set in the Reference Data endpoint, place the name of the reference set in the path to the endpoint that you want to specify. For example, to retrieve the *exampleset* reference set, use the following call:

```
/opt/qradar/bin/api_client --api /referencedata/sets/exampleset --method GET
```

### Calls with query parameters

Enter Query parameters with the following syntax:

```
--params param_name=param_value
```

For example, to get a list of all endpoints that use `httpMethod POST`, you can call `/help/capabilities`. Supply the query parameters `httpMethods` and `version`. The `httpMethods` parameter requires a JSON object. You can create a JSON object inside double quotation marks by using single quotation marks, squares brackets, and commas. For example:

```
/opt/qradar/bin/api_client --api /help/capabilities --method GET --params
httpMethods="['POST']" version="0.1"
```

To determine which parameters are query or body parameters, view the output of `--print_api`.

## Calls with body parameters

Enter body parameters in the same way that you enter query parameters, for example, `--param_name=param_value`. You must specify the content type of the body that you are sending with the `--content_type TYPE` argument. For example, when you load bulk data with a content type of **element type ALN** to an existing reference set that is named **exampleset**, type:

```
/opt/qradar/bin/api_client --api /referencedata/sets/bulkLoad/exampleset --method POST
--content_type="application/json" --params data="['value1','value2','value3']"
```

**Important:** You must specify the `--content_type` argument. If not specified, the body is sent as a query parameter, and the API call fails.

## Calls to other consoles

You can use the REST API command-line client to make API calls to a different console from the client you are running. Use the `--hostname HOSTNAME` argument to determine to which host name or IP address you want to send calls. Use the following syntax:

```
/opt/qradar/bin/api_client --api /ariel/databases --method GET --hostnameIP address
```

## Stored tokens authorization

### Inputting and storing

You can generate an authorization token on the QRadar Console that you want to call. You can then enter that authorization token into the API client to use with subsequent calls. If the authorization token is valid, the token is saved to disk in the `~/opt/qradar/bin/api_client/tokens` folder with the following file name: `hostname.token`.

### Overwriting tokens

To overwrite a token for a console, make an API call to the Console by using the `--overwrite_token` argument, and then input a new token. If the token is valid, it is saved to disk.

## User name and password authorization

Use the `--pap` argument for API client to use a password-authorized protocol to authorize your API call, and then enter a user name and password. If you do not use an authorized service token, the API client cannot save your user name and password information for use by subsequent API calls to the same host.

## API client help

Use the `./api_client -h` argument to view all options for the API client.



---

## Chapter 4. Accessing the interactive API documentation page

Use the interactive API documentation page to access technical details for the RESTful APIs and experiment with making API requests to your server.

### About this task

The API documentation user interface provides descriptions and the ability to use the following REST API interfaces:

Table 4. REST API interfaces

REST API	Description
/api/analytics	Create, update, and remove custom actions for rules.
/api/ariel	View event and flow properties, create event and flow searches, and manage searches.
/api/asset_model	Returns a list of all assets in the model. You can also list all available asset property types and saved searches, and update an asset.
/api/auth	Log out and invalidate the current session.
/api/config	View and manage tenants, domains, and QRadar extensions.
/api/gui_app_framework	Install and manage applications that are created by using the GUI Application Framework Software Development Kit.
/api/help	Returns a list of API capabilities.
/api/qvm	Retrieves assets, vulnerabilities, networks, open services, networks, and filters. You can also create or update remediation tickets.
/api/reference_data	View and manage reference data collections.
/api/scanner	View, create, or start a remote scan that is related to a scan profile.
/api/siem	View, update, and close offenses. You can also add notes and manage offense closing reasons.
/api/system	Manage server hosts, network interfaces, and firewall rules.

### Procedure

1. To access the interactive API documentation interface, enter the following URL in your web browser: `https://ConsoleIPAddress/api_doc/`.
2. Click the arrow icon beside the API version you want to use.  
5.0 is the latest version for QRadarV7.2.6.
3. Go to the endpoint that you want to access.
4. Read the endpoint documentation and complete the request parameters.
5. Click **Try it out** to send the API request to your console and receive a properly formatted HTTPS response.

**Note:** When you click **Try it out**, the action is performed on the QRadar system. Not all actions can be reversed, for example, you cannot reopen an offense after you close it.

6. Review and gather the information that you need to integrate with QRadar.

---

## Chapter 5. REST API V5.0 References

Each API reference provides information about the parameters, mime type, stability, and responses for each endpoint.

---

### Analytics endpoints

Use the references for REST API V5 analytics endpoints.

#### GET /analytics/custom\_actions/actions

Retrieves a list of available custom actions.

Table 5. GET /analytics/custom\_actions/actions resource details

<b>MIME Type</b>
application/json

Table 6. GET /analytics/custom\_actions/actions request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 7. GET /analytics/custom\_actions/actions response codes

HTTP Response Code	Unique Code	Description
200		The requested list of custom actions have been successfully retrieved.

Table 7. GET /analytics/custom\_actions/actions response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An internal server error occurred while retrieving custom actions.

## Response Description

Array of available custom actions which in turn contain the following fields:

- **id** - Number - Unique ID of the custom action within the QRadar deployment.
- **name** - String - Unique name of the custom action within the QRadar deployment.
- **description** - String - Optional description attached to the custom action.
- **interpreter** - Number - Unique ID of the custom action interpreter used by the custom action.
- **script** - Number - Unique ID of the custom action script used by the custom action.
- **parameters** - Array - Array of custom action parameters contained within the custom action. Each Custom action parameter has the following fields:
  - **name** - String - Name of the custom action parameter. Unique in the context of the parent custom action.
  - **parameter\_type** - String - Custom action parameter type. Can be either *fixed* or *dynamic*.
  - **encrypted** - Boolean - Designates whether the custom action parameter value field is stored in an encrypted state. *True* if encrypted, *false* otherwise.
  - **value** - String - Value of the custom action parameter.

## Response Sample

```
[
  {
    "description": "String",
    "id": 42,
    "interpreter": 42,
    "name": "String",
    "parameters": [
      {
        "encrypted": true,
        "name": "String",
        "parameter_type": "String",
        "value": "String"
      }
    ],
    "script": 42
  }
]
```

## POST /analytics/custom\_actions/actions

Creates a new custom action with the supplied fields.

The custom action must contain the following fields:

- **name** - *Required* - String - Unique name of the custom action within the QRadar deployment.
- **description** - *Optional* - String - Description of the custom action.

- **interpreter** - *Required* - Number - Unique ID of the custom action interpreter used by the custom action.
- **script** - *Required* - Number - Unique ID of the custom action script used by the custom action.
- **parameters** - *Required* - Array - Array of custom action parameters contained within the custom action. Each Custom action parameter must have the following fields:
  - **name** - *Required* - String - Name of the custom action parameter. Unique in the context of the parent custom action.
  - **parameter\_type** - *Required* - String - Custom action parameter type. Can be either *fixed* or *dynamic*.
  - **encrypted** - *Required* - Boolean - Designates whether the custom action parameter value field is stored in an encrypted state. *True* if encrypted, *false* otherwise.
  - **value** - *Required* - String - Value of the custom action parameter. Custom action parameters with *parameter\_type fixed* can have any value. Custom action parameters with *parameter\_type dynamic* must have values corresponding to column names in an Ariel database, for example *sourceip*. Ariel database column names are available through the `/api/ariel/databases/{database_name}` endpoint.

Table 8. POST /analytics/custom\_actions/actions resource details

<b>MIME Type</b>
application/json

Table 9. POST /analytics/custom\_actions/actions request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 10. POST /analytics/custom\_actions/actions request body details

Parameter	Data Type	MIME Type	Description	Sample
custom_action	Object	application/json	Custom action JSON object containing the supplied fields (see above for more details).	<pre>{ "description": "String", "interpreter": 42, "name": "String", "parameters": [ { "encrypted": true, "name": "String", "parameter_type": "String", "value": "String" } ], "script": 42 }</pre>

Table 11. *POST /analytics/custom\_actions/actions* response codes

HTTP Response Code	Unique Code	Description
201		A new custom action has been successfully created.
422	1005	One or more parameters are invalid in request.
500	1020	An internal server error occurred while posting custom action.

## Response Description

The newly created custom action with the following fields:

- **id** - Number - Unique ID of the custom action within the QRadar deployment.
- **name** - String - Unique name of the custom action within the QRadar deployment.
- **description** - String - Optional description attached to the custom action.
- **interpreter** - Number - Unique ID of the custom action interpreter used by the custom action.
- **script** - Number - Unique ID of the custom action script used by the custom action.
- **parameters** - Array - Array of custom action parameters contained within the custom action. Each Custom action parameter has the following fields:
  - **name** - String - Name of the custom action parameter. Unique in the context of the parent custom action.
  - **parameter\_type** - String - Custom action parameter type. Can be either *fixed* or *dynamic*.
  - **encrypted** - Boolean - Designates whether the custom action parameter value field is stored in an encrypted state. *True* if encrypted, *false* otherwise.
  - **value** - String - Value of the custom action parameter.

## Response Sample

```
{
  "description": "String",
  "id": 42,
  "interpreter": 42,
  "name": "String",
  "parameters": [
    {
      "encrypted": true,
      "name": "String",
      "parameter_type": "String",
      "value": "String"
    }
  ],
  "script": 42
}
```

## GET /analytics/custom\_actions/interpreters

Retrieves a list of available custom action interpreters.

Table 12. *GET /analytics/custom\_actions/interpreters* resource details

MIME Type
application/json

Table 13. GET /analytics/custom\_actions/interpreters request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 14. GET /analytics/custom\_actions/interpreters response codes

HTTP Response Code	Unique Code	Description
200		The requested list of custom action interpreters have been retrieved.
500	1020	An internal server error occurred while retrieving available custom action interpreters.

## Response Description

Array of available custom action interpreters, each with the following fields:

- **id** - Number - Unique ID of the custom action interpreter within the QRadar deployment.
- **name** - String - Name of the custom action interpreter.

## Response Sample

```
[
  {
    "id": 42,
    "name": "String"
  }
]
```

## GET /analytics/custom\_actions/interpreters/{interpreter\_id}

Retrieves a custom action interpreter based on supplied interpreter ID.

Table 15. GET /analytics/custom\_actions/interpreters/{interpreter\_id} resource details

MIME Type
application/json

Table 16. GET /analytics/custom\_actions/interpreters/{interpreter\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
interpreter_id	path	Required	Number (Integer)	text/plain	Number id of custom action interpreter to be retrieved.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 17. GET /analytics/custom\_actions/interpreters/{interpreter\_id} response codes

HTTP Response Code	Unique Code	Description
200		- The requested custom action interpreter has been retrieved.
404	1002	The requested custom action interpreter could not be found.
500	1020	An internal server error occurred while retrieving custom action interpreter with supplied interpreter_id.

### Response Description

A custom action interpreter with the following fields:

- **id** - Number - Unique ID of the custom action interpreter within the QRadar deployment.
- **name** - String - Name of the custom action interpreter.

### Response Sample

```
{
  "id": 42,
  "name": "String"
}
```



## GET /analytics/custom\_actions/scripts

Retrieves a list of meta-data for available custom action script files.

Table 18. GET /analytics/custom\_actions/scripts resource details

MIME Type
application/json

Table 19. GET /analytics/custom\_actions/scripts request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 20. GET /analytics/custom\_actions/scripts response codes

HTTP Response Code	Unique Code	Description
200		The requested custom action script file has been retrieved.
500	1020	An internal server error occurred while retrieving available custom action script file meta-data.

### Response Description

Array of available custom action script file meta-data, each with the following fields:

- **id** - Number - Unique ID of the custom action script file within the QRadar deployment.
- **name** - String - Name of the custom action script file.

## Response Sample

```
[
  {
    "file_name": "String",
    "id": 42
  }
]
```

## POST /analytics/custom\_actions/scripts

Creates a new custom action script file. Newly created custom action script files require a deployment before using.

Newly created custom action script files require a deployment before use. You can include an *optional* HTTP header **file\_name** that contains the custom action script file name. If not specified, the custom action script file name defaults to the script ID of the uploaded file.

Table 21. POST /analytics/custom\_actions/scripts resource details

MIME Type
application/json

Table 22. POST /analytics/custom\_actions/scripts request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 23. POST /analytics/custom\_actions/scripts request body details

Parameter	Data Type	MIME Type	Description	Sample
file	File	application/octet-stream	<i>Required.</i> The custom action script file. Must be supplied with MIME type <i>application/octet-stream</i> .	File

Table 24. POST /analytics/custom\_actions/scripts response codes

HTTP Response Code	Unique Code	Description
201		A custom action script file has been created.
500	1020	An internal server error occurred while posting custom action script file.

## Response Description

Custom action script file meta-data with the following fields:

- **id** - Number - Unique ID of the custom action script within the QRadar deployment.
- **name** - String - Name of the custom action script.

## Response Sample

```
{
  "file_name": "String",
  "id": 42
}
```

## GET /analytics/custom\_actions/actions/{action\_id}

Retrieves a custom action based on the supplied action\_id.

Table 25. GET /analytics/custom\_actions/actions/{action\_id} resource details

MIME Type
application/json

Table 26. GET /analytics/custom\_actions/actions/{action\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
action_id	path	Required	Number (Integer)	text/plain	Long id of the custom action to be retrieved.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 27. GET /analytics/custom\_actions/actions/{action\_id} response codes

HTTP Response Code	Unique Code	Description
200		The requested custom action has been successfully retrieved.
404	1002	The requested custom action could not be found.
500	1020	An internal server error occurred while retrieving custom action with supplied action_id.

## Response Description

A custom action with containing following fields:

- **id** - Number - Unique ID of the custom action within the QRadar deployment.
- **name** - String - Unique name of the custom action within the QRadar deployment.

- **description** - String - Optional description attached to the custom action.
- **interpreter** - Number - Unique ID of the custom action interpreter used by the custom action.
- **script** - Number - Unique ID of the custom action script used by the custom action.
- **parameters** - Array - Array of custom action parameters contained within the custom action. Each Custom action parameter has the following fields:
  - **name** - String - Name of the custom action parameter. Unique in the context of the parent custom action.
  - **parameter\_type** - String - Custom action parameter type. Can be either *fixed* or *dynamic*.
  - **encrypted** - Boolean - Designates whether the custom action parameter value field is stored in an encrypted state. *True* if encrypted, *false* otherwise.
  - **value** - String - Value of the custom action parameter.

### Response Sample

```
{
  "description": "String",
  "id": 42,
  "interpreter": 42,
  "name": "String",
  "parameters": [
    {
      "encrypted": true,
      "name": "String",
      "parameter_type": "String",
      "value": "String"
    }
  ],
  "script": 42
}
```

## POST /analytics/custom\_actions/actions/{action\_id}

Updates an existing custom action.

The custom action must contain the following fields:

- **id** - *Required* - Number - Unique ID of the custom action within the QRadar deployment.
- **name** - *Optional* - String - Unique name of the custom action within the QRadar deployment.
- **description** - *Optional* - String - Description of the custom action.
- **interpreter** - *Required* - Number - Unique ID of the custom action interpreter used by the custom action.
- **script** - *Required* - Number - Unique ID of the custom action script used by the custom action.
- **parameters** - *Required* - Array - Array of custom action parameters contained within the custom action. Each Custom action parameter must have the following fields:
  - **name** - *Required* - String - Name of the custom action parameter. Unique in the context of the parent custom action.
  - **parameter\_type** - *Optional* - String - Custom action parameter type. Can be either *fixed* or *dynamic*.

- **encrypted** - *Optional* - Boolean - Designates whether the custom action parameter value field is stored in an encrypted state. *True* if encrypted, *false* otherwise.
- **value** - *Optional* - String - Value of the custom action parameter. Custom action parameters with *parameter\_type fixed* can have any value. Custom action parameters with *parameter\_type dynamic* must have values corresponding to column names in an Ariel database, for example *sourceip*. Ariel database column names are available through the */api/ariel/databases/{database\_name}* endpoint.

Table 28. POST /analytics/custom\_actions/actions/{action\_id} resource details

<b>MIME Type</b>
application/json

Table 29. POST /analytics/custom\_actions/actions/{action\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
action_id	path	Required	Number (Integer)	text/plain	Number id of the custom action to be updated.
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 30. POST /analytics/custom\_actions/actions/{action\_id} request body details

Parameter	Data Type	MIME Type	Description	Sample
custom_action	Object	application/json	Custom action JSON object which can contain the supplied fields (see above for more details).	{ "description": "String", "id": 42, "interpreter": 42, "name": "String", "parameters": [ { "encrypted": true, "name": "String", "parameter_type": "String", "value": "String" } ], "script": 42 }

Table 31. POST /analytics/custom\_actions/actions/{action\_id} response codes

HTTP Response Code	Unique Code	Description
200		The custom action has been updated.
404	1002	The requested custom action could not be found.
422	1005	One or more parameters are invalid in request.
500	1020	An internal server error occurred while updating custom action with supplied action_id.

## Response Description

The updated custom action with the following fields:

- **id** - Number - Unique ID of the custom action within the QRadar deployment.
- **name** - String - Unique name of the custom action within the QRadar deployment.
- **description** - String - Optional description attached to the custom action.
- **interpreter** - Number - Unique ID of the custom action interpreter used by the custom action.
- **script** - Number - Unique ID of the custom action script used by the custom action.
- **parameters** - Array - Array of custom action parameters contained within the custom action. Each Custom action parameter has the following fields:
  - **name** - String - Name of the custom action parameter. Unique in the context of the parent custom action.
  - **parameter\_type** - String - Custom action parameter type. Can be either *fixed* or *dynamic*.
  - **encrypted** - Boolean - Designates whether the custom action parameter value field is stored in an encrypted state. *True* if encrypted, *false* otherwise.
  - **value** - String - Value of the custom action parameter.

## Response Sample

```
{
  "description": "String",
  "id": 42,
  "interpreter": 42,
  "name": "String",
  "parameters": [
    {
      "encrypted": true,
      "name": "String",
      "parameter_type": "String",
      "value": "String"
    }
  ],
  "script": 42
}
```

## DELETE /analytics/custom\_actions/actions/{action\_id}

Deletes an existing custom action.

Table 32. DELETE /analytics/custom\_actions/actions/{action\_id} resource details

MIME Type
text/plain

Table 33. DELETE /analytics/custom\_actions/actions/{action\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
action_id	path	Required	Number (Integer)	text/plain	Number id of the custom action you wish to delete.

Table 34. DELETE /analytics/custom\_actions/actions/{action\_id} response codes

HTTP Response Code	Unique Code	Description
204		The custom action has been deleted.
404	1002	The requested custom action could not be found.
500	1020	An internal server error occurred while deleting custom action with supplied action_id.

## Response Description

Empty response with 204 successful response code.

## Response Sample

### GET /analytics/custom\_actions/scripts/{script\_id}

Retrieves meta-data of a custom action script file based on supplied script\_id.

Table 35. GET /analytics/custom\_actions/scripts/{script\_id} resource details

MIME Type
application/json

Table 36. GET /analytics/custom\_actions/scripts/{script\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
script_id	path	Required	Number (Integer)	text/plain	Number id of the custom action script file.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 37. GET /analytics/custom\_actions/scripts/{script\_id} response codes

HTTP Response Code	Unique Code	Description
200		The requested custom action script file has been retrieved.
404	1002	The requested custom action script file could not be found.
500	1020	An internal server error occurred while retrieving custom action script file meta-data with supplied script_id.

## Response Description

Custom action script file meta-data with the following fields:

- **id** - Number - Unique ID of the custom action script file within the QRadar deployment.
- **name** - String - Name of the custom action script file.

## Response Sample

```
{
  "file_name": "String",
  "id": 42
}
```

## POST /analytics/custom\_actions/scripts/{script\_id}

Updates an existing custom action script file. Updated custom action script files require a deployment before using.

Updated custom action script files require a deployment before use. You can include an *optional* HTTP header **file\_name** containing the custom action script file name. If not specified, the custom action script file name defaults to the script ID of the uploaded file.

Table 38. POST /analytics/custom\_actions/scripts/{script\_id} resource details

<b>MIME Type</b>
application/json

Table 39. POST /analytics/custom\_actions/scripts/{script\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
script_id	path	Required	Number (Integer)	text/plain	Number id of the custom action script file to be updated.
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 40. POST /analytics/custom\_actions/scripts/{script\_id} request body details

Parameter	Data Type	MIME Type	Description	Sample
file	File	application/octet-stream	<i>Required.</i> The custom action script file. Must be supplied with MIME type <i>application/octet-stream</i> .	File



Table 41. POST /analytics/custom\_actions/scripts/{script\_id} response codes

HTTP Response Code	Unique Code	Description
200		The custom action script file has been updated.
404	1002	The requested custom action script file could not be found.
500	1020	An internal server error occurred while updating custom action script file with supplied script_id.

## Response Description

Custom action script file meta-data with the following fields:

- **id** - Number - Unique ID of the custom action script file within the QRadar deployment.
- **name** - String - Name of the custom action script file.

## Response Sample

```
{
  "file_name": "String",
  "id": 42
}
```

## DELETE /analytics/custom\_actions/scripts/{script\_id}

Deletes an existing custom action script file.

Table 42. DELETE /analytics/custom\_actions/scripts/{script\_id} resource details

MIME Type
text/plain

Table 43. DELETE /analytics/custom\_actions/scripts/{script\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
script_id	path	Required	Number (Integer)	text/plain	Number id of the custom action script file to be deleted.

Table 44. DELETE /analytics/custom\_actions/scripts/{script\_id} response codes

HTTP Response Code	Unique Code	Description
204		The custom action script file has been deleted.
404	1002	The requested custom action script file could not be found.
422	1005	The requested custom action script file is tied to an existing custom action.
500	1020	An internal server error occurred while deleting custom action script file with supplied script_id.

## Response Description

Empty response with a 204 successful response code.

## Response Sample

---

## Ariel endpoints

Use the references for REST API V5 Ariel endpoints.

### GET /ariel/databases

Retrieve Ariel database names

Retrieve a list of available Ariel databases.

Table 45. GET /ariel/databases resource details

<b>MIME Type</b>
application/json

Table 46. GET /ariel/databases request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 47. GET /ariel/databases response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of Ariel databases.

## Response Description

The names of the available Ariel databases.

## Response Sample

```
[  
  "String"  
]
```

## GET /ariel/databases/{database\_name}

Retrieve the columns defined for a specific Ariel database.

This is the set of columns that can be explicitly named in the column list of a SELECT query.

Table 48. GET /ariel/databases/{database\_name} resource details

<b>MIME Type</b>
application/json

Table 49. GET /ariel/databases/{database\_name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
database_name	path	Required	String	text/plain	Required. The name of the Ariel database that contains the columns that you want to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 50. GET /ariel/databases/{database\_name} response codes

HTTP Response Code	Unique Code	Description
200		The database columns were retrieved.
404	1002	The database does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the database columns.

### Response Description

A list of columns that are defined for the specified database. Multiple properties of each column are returned. For example, the column name or an indication that the column is indexable.

## Response Sample

```
{
  "columns": [
    {
      "argument_type": "String",
      "indexable": true,
      "name": "String"
    }
  ]
}
```

## GET /ariel/searches

Retrieve Ariel search\_ids.

Retrieve the list of Ariel searches. This includes search\_ids for completed and active searches.

Table 51. GET /ariel/searches resource details

MIME Type
application/json

Table 52. GET /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 53. GET /ariel/searches response codes

HTTP Response Code	Unique Code	Description
200		The search list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of searches.

## Response Description

A list of search IDs.

## Response Sample

```
[
  "String"
]
```

## POST /ariel/searches

Create a new asynchronous Ariel search

Creates a new Ariel search as specified by the Ariel Query Language (AQL) query expression. Searches are executed asynchronously. A reference to the search\_id is returned and should be used in subsequent API calls to determine the status of the search and retrieve the results once it is complete.

This endpoint only accepts SELECT and RUN query expressions.

Queries are applied to the range of data in a certain time interval. By default this time interval is the last 60 seconds. An alternative time interval can be specified by specifying them as part of the query expression. For further information, see the AQL reference.

Table 54. POST /ariel/searches resource details

<b>MIME Type</b>
application/json

Table 55. POST /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
query_expression	query	Required	String	text/plain	Required - The AQL query to execute.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 56. POST /ariel/searches response codes

HTTP Response Code	Unique Code	Description
201		A new Ariel search was successfully created.
409	1004	The search could not be created, the requested search ID provided in the query_expression is already in use. Please use a unique search ID (or allow one to be generated).
422	2000	The query_expression contains invalid AQL syntax.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create a new search.

### Response Description

Information about the specified search, including the search\_id. Use the search\_id to access or manipulate the search with the other API endpoints.

If the exact search being created was already recently created, the response message will return a reference to the original search\_id rather than creating a new search.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## GET /ariel/searches/{search\_id}

Retrieve information about an Ariel search

Retrieve status information for a search, based on the **search\_id** parameter. The same informational fields are returned regardless of whether the search is in progress or is complete.

Table 57. GET /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 58. GET /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The identifier for an Ariel search.

Table 58. GET /ariel/searches/{search\_id} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 59. GET /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search information was retrieved.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search information.

## Response Description

Information about the specified search, including the search status.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## POST /ariel/searches/{search\_id}

Update an Ariel search.

Update details for an Ariel search. You can update searches in the following ways:

- To cancel an active search, set the **status** parameter to CANCELED. This stops the search and keeps any search results that were collected before the search was canceled.
- The results for a completed search can be saved by setting the **save\_results** parameter to true. This ensures that the search is not automatically removed when it expires in accordance with the retention policy.

The Ariel server uses an internal retention policy to manage available disk space. Searches might be deleted automatically, according to the settings of the retention policy. Searches with saved results are not automatically reclaimed by the server and are therefore retained. A search can be explicitly deleted by using the DELETE /searches/{search\_id} endpoint.

**Note:** Saving too many search results might result in insufficient disk space to process new searches.

Table 60. POST /ariel/searches/{search\_id} resource details

<b>MIME Type</b>
application/json

Table 61. POST /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The ID of the search to update.
save_results	query	Optional	String	text/plain	Optional. The only accepted value is true. If this value is provided, the search results will not be deleted by the search expiration removal process.
status	query	Optional	String	text/plain	Optional. The only accepted value is CANCELED. If this value is provided, the search will be canceled.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.



Table 62. POST /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search was updated.
404	1002	The search does not exist.
409	1008	The current status of the search prevented the search results from being saved.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to update the search.

## Response Description

Information about the specified search that was updated.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## DELETE /ariel/searches/{search\_id}

Delete an Ariel search

Deletes an Ariel search. This discards any results that were collected and stops the search if it is currently processing. This search is deleted regardless of whether the results were saved.

Table 63. DELETE /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 64. DELETE /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required - The search_id of the search to delete.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 65. DELETE /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
202		The delete request has been accepted.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to delete the search.

## Response Description

Information about the deleted search

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
}
```

```

    "save_results": true,
    "search_id": "String",
    "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
  }

```

## GET /ariel/searches/{search\_id}/results

Retrieves search results in the requested format.

Retrieve the results of the Ariel search that is identified by the search\_id. The Accepts request header indicates the format of the result. The format can be JSON, CSV, XML, or tabular text.

By default, all query result records are returned. To restrict the results to a contiguous subset of the records, you can supply a Range header to specify the inclusive range of records to be returned.

This end-point works with query results that are generated by AQL query expressions. This endpoint might not work as expected for results that are generated by other means. Search results might not be retrievable for searches that are created on the Console.

The response samples are for the following query: Select sourceIP, destinationIP from events.

Table 66. GET /ariel/searches/{search\_id}/results resource details

MIME Type
application/json application/csv text/table application/xml

Table 67. GET /ariel/searches/{search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	The ID of the search criteria for the returned results.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 68. GET /ariel/searches/{search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The search results were retrieved.
404	1002	The search does not exist.
404	1003	Search results not found. The search is still in progress.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search results.

## Response Description

The search results for the specified search\_id. The format that is used to encapsulate the data depends on the format specified in the Accept header for this request.

## Response Sample

```
{
  "events": [
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    },
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    }
  ]
}
```

---

## Asset model endpoints

Use the references for REST API V5 Asset Model endpoints.

### GET /asset\_model/assets

List all assets found in the model.

Table 69. GET /asset\_model/assets resource details

<b>MIME Type</b>
application/json

Table 70. GET /asset\_model/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 70. GET /asset\_model/assets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 71. GET /asset\_model/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
500	1020	The server encountered an error while trying to retrieve the assets.

## Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[{"id": 42,
  "domain_id": 42,
  "interfaces": [{"first_seen_scanner": 42,
    "id": 42,
    "first_seen_profiler": 42,
    "created": 42,
    "last_seen_profiler": 42,
    "last_seen_scanner": 42,
    "mac_address": "String",
    "ip_addresses": [{"first_seen_scanner": 42,
      "id": 42,
      "first_seen_profiler": 42,
      "created": 42,
      "network_id": 42,
      "value": "String",
      "last_seen_profiler": 42,
      "last_seen_scanner": 42,
      "type": "String"}]
    }],
  "properties": [{"id": 42,
    "name": "String",
    "value": "String",
    "last_reported": 42,
    "type_id": 42,
    "last_reported_by": "String"}]
}]
```

## POST /asset\_model/assets/{asset\_id}

Update an asset with several pertinent pieces of information.

The **asset\_id** tag is mandatory, and is the unique identifier for an asset. This field is available through the `/asset_model/assets` or `/asset_model/saved_searches/{saved_search_id}/results` query. To update properties, the property type ID which

is available through the `/asset_model/properties` query must be provided along with the new value. See the sample provided demonstrating an example asset update.

Table 72. `POST /asset_model/assets/{asset_id}` resource details

<b>MIME Type</b>
text/plain

Table 73. `POST /asset_model/assets/{asset_id}` request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
asset_id	path	Required	String	text/plain	Unique identifier of the asset to update.

Table 74. `POST /asset_model/assets/{asset_id}` request body details

Parameter	Data Type	MIME Type	Description	Sample
asset	JSON	application/json	JSON representation of an asset.	{ "properties": [ { "type_id": 1001, "value": "given name value" }, { "type_id": 1002, "value": "unified name value" } ] }

Table 75. `POST /asset_model/assets/{asset_id}` response codes

HTTP Response Code	Unique Code	Description
202		The request to update the asset was successful. The update will take place when the asset profile application receives the request.
422	1005	One or more of the requested property updates were invalid.
500	1020	The server encountered an error registering the update with the asset profile application.

## Response Description

Information about the asset that was updated.

## Response Sample

String

## GET /asset\_model/properties

Get a list of available asset property types that can be used.

Get a list of available asset property types that can be used or applied against the `/asset_model/assets` endpoint.

Table 76. `GET /asset_model/properties` resource details

<b>MIME Type</b>
application/json

Table 77. GET /asset\_model/properties request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 78. GET /asset\_model/properties response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of asset property types completed successfully.
500	1020	An error occurred while trying to retrieve the list of asset property types.

## Response Description

List of asset properties. Per asset property type: id and name that make up this asset property type.

## Response Sample

```
[
  {
    "custom": true,
    "data_type": "String",
    "display": true,
    "id": 42,
    "name": "String",
    "state": 42
  }
]
```

## GET /asset\_model/saved\_searches

Get a list of saved searches that can be used.

Get a list of saved searches that can be used or applied against the `/asset_model/saved_searches/{saved_search_id}/results` query.

Table 79. GET /asset\_model/saved\_searches resource details

<b>MIME Type</b>
application/json

Table 80. GET /asset\_model/saved\_searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 81. GET /asset\_model/saved\_searches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully.
500	1020	The server encountered an error while trying to retrieve the list of saved searches.

## Response Description

List of saved searches. Per saved search: id, name and list of filters that make up this saved search

## Response Sample

```
[
  {
    "columns": [
      {
        "name": "String",
```



```

        "type": "String"
      }
    ],
    "description": "String",
    "filters": [
      {
        "operator": "String",
        "parameter": "String",
        "value": "String"
      }
    ],
    "id": 42,
    "name": "String"
  }
]

```

## GET /asset\_model/saved\_searches/{saved\_search\_id}/results

Retrieves a list of assets based on the results of an asset saved search.

Table 82. GET /asset\_model/saved\_searches/{saved\_search\_id}/results resource details

MIME Type
application/json

Table 83. GET /asset\_model/saved\_searches/{saved\_search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
saved_search_id	path	Required	String	text/plain	Unique identifier of the saved search used to retrieve assets.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 84. GET /asset\_model/saved\_searches/{saved\_search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
422	1005	The unique identifier of the saved search provided was invalid.

Table 84. GET /asset\_model/saved\_searches/{saved\_search\_id}/results response codes (continued)

HTTP Response Code	Unique Code	Description
500	1003	The server encountered an error executing the saved search.

## Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[
  {
    "domain_id": 42,
    "id": 42,
    "interfaces": [
      {
        "created": 42,
        "first_seen_profiler": 42,
        "first_seen_scanner": 42,
        "id": 42,
        "ip_addresses": [
          {
            "created": 42,
            "first_seen_profiler": 42,
            "first_seen_scanner": 42,
            "id": 42,
            "last_seen_profiler": 42,
            "last_seen_scanner": 42,
            "network_id": 42,
            "type": "String",
            "value": "String"
          }
        ],
        "last_seen_profiler": 42,
        "last_seen_scanner": 42,
        "mac_address": "String"
      }
    ],
    "properties": [
      {
        "id": 42,
        "last_reported": 42,
        "last_reported_by": "String",
        "name": "String",
        "type_id": 42,
        "value": "String"
      }
    ]
  }
]
```

---

## Authentication endpoints

Use the references for REST API V5 authentication endpoints.

## POST /auth/logout

Invoke this method as an authorized user and your session will be invalidated.

Table 85. POST /auth/logout resource details

MIME Type
text/plain

There are no parameters for this endpoint.

Table 86. POST /auth/logout response codes

HTTP Response Code	Unique Code	Description
200		The session was invalidated.

### Response Description

Returns true. Throws exception upon failure.

### Response Sample

```
true
```

---

## Configuration endpoints

Use the references for REST API V5 configuration endpoints.

## GET /config/domain\_management/domains

Retrieves the list of all domains, active and deleted (including the default domain).

The list is ordered by domain ID. If domains were never configured, only the default domain is returned.

Table 87. GET /config/domain\_management/domains resource details

MIME Type
application/json

Table 88. GET /config/domain\_management/domains request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 88. GET /config/domain\_management/domains request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 89. GET /config/domain\_management/domains response codes

HTTP Response Code	Unique Code	Description
200		The domain list has been successfully retrieved.
500	1020	An error occurred while the domain list was being retrieved.

## Response Description

The list of domain objects.

## Response Sample

```
[
  {
    "asset_scanner_ids": [
      42
    ],
    "custom_properties": [
      {
        "capture_result": "String",
        "id": 42
      }
    ],
    "deleted": true,
    "description": "String",
    "event_collector_ids": [
      42
    ],
    "flow_collector_ids": [
      42
    ],
    "flow_source_ids": [
      42
    ],
    "id": 42,
    "log_source_group_ids": [
      42
    ]
  }
]
```

```

    ],
    "log_source_ids": [
        42
    ],
    "name": "String",
    "qvm_scanner_ids": [
        42
    ],
    "tenant_id": 42
}
]

```

## POST /config/domain\_management/domains

Creates a new domain.

Table 90. POST /config/domain\_management/domains resource details

<b>MIME Type</b>
application/json

Table 91. POST /config/domain\_management/domains request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 92. POST /config/domain\_management/domains request body details

Parameter	Data Type	MIME Type	Description	Sample
domain	Object	application/json	A domain JSON object (its <i>id</i> parameter is ignored).	{ "asset_scanner_ids": [42], "custom_properties": [{"capture_result": "String", "id": 42}], "deleted": true, "description": "String", "event_collector_ids": [42], "flow_collector_ids": [42], "flow_source_ids": [42], "log_source_group_ids": [42], "log_source_ids": [42], "name": "String", "qvm_scanner_ids": [42], "tenant_id": 42 }

Table 93. POST /config/domain\_management/domains response codes

HTTP Response Code	Unique Code	Description
201		The domain has been successfully created.

Table 93. *POST /config/domain\_management/domains response codes (continued)*

HTTP Response Code	Unique Code	Description
409	1004	A domain object parameter already exists.
422	1005	A domain object parameter is invalid.
500	1020	An error occurred while the domain was being created.

## Response Description

A created domain object.

## Response Sample

```
{
  "asset_scanner_ids": [
    42
  ],
  "custom_properties": [
    {
      "capture_result": "String",
      "id": 42
    }
  ],
  "deleted": true,
  "description": "String",
  "event_collector_ids": [
    42
  ],
  "flow_collector_ids": [
    42
  ],
  "flow_source_ids": [
    42
  ],
  "id": 42,
  "log_source_group_ids": [
    42
  ],
  "log_source_ids": [
    42
  ],
  "name": "String",
  "qvm_scanner_ids": [
    42
  ],
  "tenant_id": 42
}
```

## GET /config/domain\_management/domains/{domain\_id}

Retrieves a domain by domain ID.

Table 94. *GET /config/domain\_management/domains/{domain\_id} resource details*

MIME Type
application/json

Table 95. GET /config/domain\_management/domains/{domain\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
domain_id	path	Required	Number (Integer)	text/plain	The ID of the domain object to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 96. GET /config/domain\_management/domains/{domain\_id} response codes

HTTP Response Code	Unique Code	Description
200		The domain has been successfully retrieved.
404	1002	No domain was found for the provided domain id.
500	1020	An error occurred while the domain was being retrieved.

## Response Description

A domain object.

## Response Sample

```
{
  "asset_scanner_ids": [
    42
  ],
  "custom_properties": [
    {
      "capture_result": "String",
      "id": 42
    }
  ],
  "deleted": true,
  "description": "String",
  "event_collector_ids": [
    42
  ],
  "flow_collector_ids": [
    42
  ],
  "flow_source_ids": [
    42
  ],
  "id": 42,
  "log_source_group_ids": [
    42
  ],
  "log_source_ids": [
    42
  ],
}
```

```

    "name": "String",
    "qvm_scanner_ids": [
      42
    ],
    "tenant_id": 42
  }

```

## POST /config/domain\_management/domains/{domain\_id}

Updates an existing domain.

Table 97. POST /config/domain\_management/domains/{domain\_id} resource details

MIME Type
application/json

Table 98. POST /config/domain\_management/domains/{domain\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
domain_id	path	Required	Number (Integer)	text/plain	The ID of the domain object to update.
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 99. POST /config/domain\_management/domains/{domain\_id} request body details

Parameter	Data Type	MIME Type	Description	Sample
domain	Object	application/json	A domain JSON object.	{ "asset_scanner_ids": [42], "custom_properties": [{"capture_result": "String", "id": 42}], "deleted": true, "description": "String", "event_collector_ids": [42], "flow_collector_ids": [42], "flow_source_ids": [42], "log_source_group_ids": [42], "log_source_ids": [42], "name": "String", "qvm_scanner_ids": [42], "tenant_id": 42 }

Table 100. POST /config/domain\_management/domains/{domain\_id} response codes

HTTP Response Code	Unique Code	Description
200		The domain has been successfully updated.



Table 100. *POST /config/domain\_management/domains/{domain\_id}* response codes (continued)

HTTP Response Code	Unique Code	Description
404	1002	No domain was found for the provided domain id.
409	1004	A domain object parameter already exists.
422	1005	A domain object parameter is invalid.
500	1020	An error occurred while the domain was being updated.

## Response Description

The updated domain object.

## Response Sample

```
{
  "asset_scanner_ids": [
    42
  ],
  "custom_properties": [
    {
      "capture_result": "String",
      "id": 42
    }
  ],
  "deleted": true,
  "description": "String",
  "event_collector_ids": [
    42
  ],
  "flow_collector_ids": [
    42
  ],
  "flow_source_ids": [
    42
  ],
  "id": 42,
  "log_source_group_ids": [
    42
  ],
  "log_source_ids": [
    42
  ],
  "name": "String",
  "qvm_scanner_ids": [
    42
  ],
  "tenant_id": 42
}
```

## DELETE /config/domain\_management/domains/{domain\_id}

Deletes a domain by domain ID.

All domain mappings are also deleted

Table 101. *DELETE /config/domain\_management/domains/{domain\_id}* resource details

MIME Type
application/json

Table 102. DELETE /config/domain\_management/domains/{domain\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
domain_id	path	Required	Number (Integer)	text/plain	The ID of the domain object to delete.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 103. DELETE /config/domain\_management/domains/{domain\_id} response codes

HTTP Response Code	Unique Code	Description
200		The domain has been successfully deleted.
404	1002	No domain was found for the provided domain id.
422	1005	Default domain cannot be deleted.
500	1020	An error occurred while the domain was being deleted.

## Response Description

The deleted domain object with its parameter *deleted* set to true.

## Response Sample

```
{
  "asset_scanner_ids": [
    42
  ],
  "custom_properties": [
    {
      "capture_result": "String",
      "id": 42
    }
  ],
  "deleted": true,
  "description": "String",
  "event_collector_ids": [
    42
  ],
  "flow_collector_ids": [
    42
  ],
  "flow_source_ids": [
    42
  ],
  "id": 42,
  "log_source_group_ids": [
```

```

    42
  ],
  "log_source_ids": [
    42
  ],
  "name": "String",
  "qvm_scanner_ids": [
    42
  ],
  "tenant_id": 42
}

```

## GET /config/access/tenant\_management/tenants

Retrieve the list of all tenants ordered by tenant ID.

Retrieve the list of all tenants. The list is ordered by tenant ID.

Table 104. GET /config/access/tenant\_management/tenants resource details

<b>MIME Type</b>
application/json

Table 105. GET /config/access/tenant\_management/tenants request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 106. GET /config/access/tenant\_management/tenants response codes

HTTP Response Code	Unique Code	Description
200		The tenant list was successfully retrieved.
500	1020	An error occurred while the tenant list was being retrieved.

## Response Description

a list of all the tenants

## Response Sample

```
[
  {
    "deleted": true,
    "description": "String",
    "event_rate_limit": 42,
    "flow_rate_limit": 42,
    "id": 42,
    "name": "String"
  }
]
```

## POST /config/access/tenant\_management/tenants

Create a new tenant.

Table 107. POST /config/access/tenant\_management/tenants resource details

MIME Type
application/json

Table 108. POST /config/access/tenant\_management/tenants request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 109. POST /config/access/tenant\_management/tenants request body details

Parameter	Data Type	MIME Type	Description	Sample
tenant	Object	application/json	Required - Tenant - includes name, event_rate_limit (unit eps), flow_rate_limit (unit fpm) and description	{ "deleted": true, "description": "String", "event_rate_limit": 42, "flow_rate_limit": 42, "name": "String" }

Table 110. POST /config/access/tenant\_management/tenants response codes

HTTP Response Code	Unique Code	Description
201		A new tenant was created successfully and returned the new tenant object.
409	1004	A tenant with the given name already exists.
422	1005	A request parameter is invalid.

Table 110. POST /config/access/tenant\_management/tenants response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	Failed to create the tenant.

## Response Description

a created tenant object

## Response Sample

```
{
  "deleted": true,
  "description": "String",
  "event_rate_limit": 42,
  "flow_rate_limit": 42,
  "id": 42,
  "name": "String"
}
```

## GET /config/access/tenant\_management/tenants/{tenant\_id}

Retrieve a tenant by tenant id.

Table 111. GET /config/access/tenant\_management/tenants/{tenant\_id} resource details

MIME Type
application/json

Table 112. GET /config/access/tenant\_management/tenants/{tenant\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
tenant_id	path	Required	Number (Integer)	text/plain	null
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 113. GET /config/access/tenant\_management/tenants/{tenant\_id} response codes

HTTP Response Code	Unique Code	Description
200		The tenant was successfully retrieved.
404	1002	No tenant was found for the provided tenant id.
500	1020	An error occurred while the tenant was being retrieved.

## Response Description

the associated tenants object

## Response Sample

```
{
  "deleted": true,
  "description": "String",
  "event_rate_limit": 42,
  "flow_rate_limit": 42,
  "id": 42,
  "name": "String"
}
```

## POST /config/access/tenant\_management/tenants/{tenant\_id}

Update a tenant

Table 114. POST /config/access/tenant\_management/tenants/{tenant\_id} resource details

MIME Type
application/json

Table 115. POST /config/access/tenant\_management/tenants/{tenant\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
tenant_id	path	Required	Number (Integer)	text/plain	Required - Integer - the tenant id to modify
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 116. POST /config/access/tenant\_management/tenants/{tenant\_id} request body details

Parameter	Data Type	MIME Type	Description	Sample
tenant	Object	application/json	Required - Tenant - includes name, event_rate_limit (unit eps), flow_rate_limit (unit fpm) and description	{ "deleted": true, "description": "String", "event_rate_limit": 42, "flow_rate_limit": 42, "name": "String" }

Table 117. POST /config/access/tenant\_management/tenants/{tenant\_id} response codes

HTTP Response Code	Unique Code	Description
200		A tenant profile that was updated successfully and returned the updated tenant object.

Table 117. POST /config/access/tenant\_management/tenants/{tenant\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1002	The tenant profile does not exist.
409	1004	A tenant with the given name already exists.
422	1005	A request parameter is invalid.
500	1020	Failed to retrieve/update the given tenant profile.

## Response Description

the updated tenant object

## Response Sample

```
{
  "deleted": true,
  "description": "String",
  "event_rate_limit": 42,
  "flow_rate_limit": 42,
  "id": 42,
  "name": "String"
}
```

## DELETE /config/access/tenant\_management/tenants/{tenant\_id}

Delete a tenant.

Deletes a tenant by tenant ID.

Table 118. DELETE /config/access/tenant\_management/tenants/{tenant\_id} resource details

MIME Type
application/json

Table 119. DELETE /config/access/tenant\_management/tenants/{tenant\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
tenant_id	path	Required	Number (Integer)	text/plain	Required - String - id associated to a tenant

Table 120. DELETE /config/access/tenant\_management/tenants/{tenant\_id} response codes

HTTP Response Code	Unique Code	Description
200		The tenant was deleted successfully (soft delete).
404	1002	The tenant does not exist.
500	1020	An error occurred while deleting tenant.

## Response Description

the deleted tenant object with its parameter *deleted* set to true

## Response Sample

```
{
  "deleted": true,
  "description": "String",
  "event_rate_limit": 42,
  "flow_rate_limit": 42,
  "id": 42,
  "name": "String"
}
```

## GET /config/extension\_management/extensions

Retrieve a list of extensions.

Table 121. GET /config/extension\_management/extensions resource details

MIME Type
application/json

Table 122. GET /config/extension\_management/extensions request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
sort	query	Optional	String	text/plain	Optional - This parameter is used to sort the elements in a list.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 123. GET /config/extension\_management/extensions response codes

HTTP Response Code	Unique Code	Description
200		The requested list of extensions has been retrieved.
422	22608	The supplied filter is invalid.



Table 123. GET /config/extension\_management/extensions response codes (continued)

HTTP Response Code	Unique Code	Description
422	22615	Unknown status used in filter.
422	22610	The selected field cannot be utilized for sorting.
422	22609	Only top-level-elements of the root entity can be sorted on.
500	22602	An error has occurred while trying to retrieve the list of extensions.

## Response Description

A list of extensions. Each extension contains the following fields:

- **id** - Number - Unique ID of this extension within the QRadar deployment.
- **name** - String - The name of the extension.
- **description** - String - The description of the extension.
- **author** - String - The author (person who generated) the extension.
- **version** - String - The version of the extension.
- **supported\_languages** - Array of strings - The language tags supported by this extension.
- **exported\_qradar\_version** - String - The version of the QRadar deployment this extension was exported from.
- **min\_qradar\_version** - String - The minimum QRadar version required for the extension to function properly.
- **file\_location** - String - The location of the extension file on disk.
- **size** - Number - The size in bytes of the extension file.
- **signed** - String - The state of the extension's signature.
- **beta** - Boolean - True if the extension is considered to be beta or experimental.
- **added\_by** - String - The user or authorized service that added the extension to QRadar.
- **installed\_by** - String - The user or authorized service that installed the extension.
- **add\_time** - Number - The date/time at which the extension was added to QRadar, represented as number of milliseconds since Unix epoch.
- **install\_time** - Number - The date/time at which the extension was installed, represented as number of milliseconds since Unix epoch.
- **full\_uninstall** - Boolean - True if the extension and all of its contents can be fully uninstalled.
- **status** - String - The tag corresponding to the current status of the extension. Possible values are UPLOADED, UPLOADING, INSTALLED, INSTALLING, INSTALL\_FAILED, UNINSTALLED, UNINSTALLING, UNINSTALL\_FAILED, NOT\_INSTALLED, PREVIEWING, NONE.
- **contents** - Array of objects representing an item contained within the extension. Each object has the following fields:
  - **content\_type\_id** - Number - The ID of the content type.
  - **content\_type\_name** - String - The name of the content type.
  - **identifier** - String - The descriptive name/identifier of the item.

## Response Sample

```
[
  {
    "file_location": "/store/cmt/exports/custom_rule.zip",
    "supported_languages": [
      "en_US"
    ],
    "contents": [
      {
        "content_type_id": 3,
        "identifier": "No Description Supplied",
        "content_type_name": "custom_rule"
      },
      {
        "content_type_id": 28,
        "identifier": "Asset Reconciliation IPv4 Blacklist",
        "content_type_name": "reference_data"
      },
      {
        "content_type_id": 28,
        "identifier": "Asset Reconciliation IPv4 Whitelist",
        "content_type_name": "reference_data"
      },
      {
        "content_type_id": 32,
        "identifier": "No Description Supplied",
        "content_type_name": "reference_data_rules"
      }
    ],
    "status": "INSTALLED",
    "signed": "NOT_SIGNED",
    "full_uninstall": false,
    "min_qradar_version": null,
    "beta": false,
    "version": "7.2.6.20150825133843",
    "size": 8575,
    "id": 59,
    "author": "admin",
    "description": null,
    "exported_qradar_version": null,
    "name": "custom_rule.xml",
    "install_time": 1440788704856,
    "installed_by": "admin",
    "added_by": "admin",
    "add_time": 1440693660702
  },
  {
    "file_location": "/store/cmt/exports/qidmap.xml",
    "supported_languages": [
      "en_US"
    ],
    "contents": [
      {
        "content_type_id": 27,
        "identifier": "",
        "content_type_name": "qidmap"
      }
    ],
    "status": "INSTALLED",
    "signed": "NOT_SIGNED",
    "full_uninstall": false,
    "min_qradar_version": null,
    "beta": false,
    "version": "7.2.6.20150821144442",
    "size": 675,
    "id": 2,
    "author": "admin",
  }
]
```

```

    "description": null,
    "exported_qradar_version": null,
    "name": "qidmap.xml",
    "install_time": 1440612194941,
    "installed_by": "admin",
    "added_by": "admin",
    "add_time": 1440555001236
  }
]

```

## POST /config/extension\_management/extensions

Uploads the supplied extension file to the IBM Security QRadar system.

Table 124. POST /config/extension\_management/extensions resource details

MIME Type
application/json

Table 125. POST /config/extension\_management/extensions request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 126. POST /config/extension\_management/extensions request body details

Parameter	Data Type	MIME Type	Description	Sample
file	File	application/x-gzip	Required - The Extension file. Must be a properly-formed QRadar extension/content export, either an XML file or an XML within a ZIP or TAR.GZ archive. Must be provided with MIME type application/xml, application/zip, application/x-gzip or multipart/form-data	File

Table 127. POST /config/extension\_management/extensions response codes

HTTP Response Code	Unique Code	Description
201		The supplied extension file has been uploaded.
409	22613	The supplied extension file can not be uploaded because it shares the same hub_id and version as one of the extensions in the system.

Table 127. *POST /config/extension\_management/extensions response codes (continued)*

HTTP Response Code	Unique Code	Description
422	22607	The supplied extension could not be validated successfully
422	22616	The supplied manifest for the extension is invalid.
500	22602	An error has occurred while trying to upload the extension file.

## Response Description

An extension containing the following fields:

- **id** - Number - Unique ID of this extension within the QRadar deployment.
- **name** - String - The name of the extension.
- **description** - String - The description of the extension.
- **author** - String - The author (person who generated) the extension.
- **version** - String - The version of the extension.
- **supported\_languages** - Array of strings - The language tags supported by this extension.
- **exported\_qradar\_version** - String - The version of the QRadar deployment this extension was exported from.
- **min\_qradar\_version** - String - The minimum QRadar version required for the extension to function properly.
- **file\_location** - String - The location of the extension file on disk.
- **size** - Number - The size in bytes of the extension file.
- **signed** - String - The state of the extension's signature.
- **beta** - Boolean - True if the extension is considered to be beta or experimental.
- **added\_by** - String - The user or authorized service that added the extension to QRadar.
- **installed\_by** - String - The user or authorized service that installed the extension.
- **add\_time** - Number - The date/time at which the extension was added to QRadar, represented as number of milliseconds since Unix epoch.
- **install\_time** - Number - The date/time at which the extension was installed, represented as number of milliseconds since Unix epoch.
- **full\_uninstall** - Boolean - True if the extension and all of its contents can be fully uninstalled.
- **status** - String - The tag corresponding to the current status of the extension. Possible values are UPLOADED, UPLOADING, INSTALLED, INSTALLING, INSTALL\_FAILED, UNINSTALLED, UNINSTALLING, UNINSTALL\_FAILED, NOT\_INSTALLED, PREVIEWING, NONE.
- **contents** - Array of objects representing an item contained within the extension. Each object has the following fields:
  - **content\_type\_id** - Number - The ID of the content type.
  - **content\_type\_name** - String - The name of the content type.
  - **identifier** - String - The descriptive name/identifier of the item.

## Response Sample

```
{
  "file_location": "/store/cmt/exports/qidmaps.xml",
  "supported_languages": [
    "en_US"
  ],
  "contents": [
    {
      "content_type_id": 27,
      "identifier": "",
      "content_type_name": "qidmap"
    }
  ],
  "status": "INSTALLED",
  "signed": "NOT_SIGNED",
  "full_uninstall": false,
  "min_gradar_version": null,
  "beta": false,
  "version": "7.2.6.20150821144442",
  "size": 675,
  "id": 2,
  "author": "admin",
  "description": null,
  "exported_gradar_version": null,
  "name": "qidmaps.xml",
  "install_time": 1440612194941,
  "installed_by": "admin",
  "added_by": "admin",
  "add_time": 1440555001236
}
```

## GET /config/extension\_management/extensions/{extension\_id}

Retrieves an extension based on the supplied extension ID.

Table 128. GET /config/extension\_management/extensions/{extension\_id} resource details

MIME Type
application/json

Table 129. GET /config/extension\_management/extensions/{extension\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
extension_id	path	Required	Number (Integer)	text/plain	Required - The id of the extension.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 130. GET /config/extension\_management/extensions/{extension\_id} response codes

HTTP Response Code	Unique Code	Description
200		The requested extension has been retrieved.

Table 130. GET /config/extension\_management/extensions/{extension\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
404	22603	The requested extension cannot be found.
422	22606	A supplied numeric parameter was not positive.
500	22602	An error has occurred while trying to retrieve the requested extension.

## Response Description

An extension containing the following fields:

- **id** - Number - Unique ID of this extension within the QRadar deployment.
- **name** - String - The name of the extension.
- **description** - String - The description of the extension.
- **author** - String - The author (person who generated) the extension.
- **version** - String - The version of the extension.
- **supported\_languages** - Array of strings - The language tags supported by this extension.
- **exported\_qradar\_version** - String - The version of the QRadar deployment this extension was exported from.
- **min\_qradar\_version** - String - The minimum QRadar version required for the extension to function properly.
- **file\_location** - String - The location of the extension file on disk.
- **size** - Number - The size in bytes of the extension file.
- **signed** - String - The state of the extension's signature.
- **beta** - Boolean - True if the extension is considered to be beta or experimental.
- **added\_by** - String - The user or authorized service that added the extension to QRadar.
- **installed\_by** - String - The user or authorized service that installed the extension.
- **add\_time** - Number - The date/time at which the extension was added to QRadar, represented as number of milliseconds since Unix epoch.
- **install\_time** - Number - The date/time at which the extension was installed, represented as number of milliseconds since Unix epoch.
- **full\_uninstall** - Boolean - True if the extension and all of its contents can be fully uninstalled.
- **status** - String - The tag corresponding to the current status of the extension. Possible values are UPLOADED, UPLOADING, INSTALLED, INSTALLING, INSTALL\_FAILED, UNINSTALLED, UNINSTALLING, UNINSTALL\_FAILED, NOT\_INSTALLED, PREVIEWING, NONE.
- **contents** - Array of objects representing an item contained within the extension. Each object has the following fields:
  - **content\_type\_id** - Number - The ID of the content type.
  - **content\_type\_name** - String - The name of the content type.
  - **identifier** - String - The descriptive name/identifier of the item.

## Response Sample

```
{
  "file_location": "/store/cmt/exports/qidmaps.xml",
  "supported_languages": [
    "en_US"
  ],
  "contents": [
    {
      "content_type_id": 27,
      "identifier": "",
      "content_type_name": "qidmap"
    }
  ],
  "status": "INSTALLED",
  "signed": "NOT_SIGNED",
  "full_uninstall": false,
  "min_gradar_version": null,
  "beta": false,
  "version": "7.2.6.20150821144442",
  "size": 675,
  "id": 2,
  "author": "admin",
  "description": null,
  "exported_gradar_version": null,
  "name": "qidmaps.xml",
  "install_time": 1440612194941,
  "installed_by": "admin",
  "added_by": "admin",
  "add_time": 1440555001236
}
```

## POST /config/extension\_management/extensions/{extension\_id}

Install an extension based on the supplied extension ID. This is an asynchronous action.

Installs the Extension corresponding to the supplied extension ID Alternatively can be used to preview an extension, showing what values are applied if the extension is installed.

Table 131. POST /config/extension\_management/extensions/{extension\_id} resource details

MIME Type
application/json

Table 132. POST /config/extension\_management/extensions/{extension\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
extension_id	path	Required	Number (Integer)	text/plain	Required - The id of the extension.
action_type	query	Required	String	text/plain	Required - The desired action to take on the Extension (INSTALL or PREVIEW)

Table 132. *POST /config/extension\_management/extensions/{extension\_id} request parameter details (continued)*

Parameter	Type	Optionality	Data Type	MIME Type	Description
overwrite	query	Optional	Boolean	text/plain	Optional - If true, any existing items on the importing system will be overwritten if the extension contains the same items. If false, existing items will be preserved, and the corresponding items in the extension will be skipped.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 133. *POST /config/extension\_management/extensions/{extension\_id} response codes*

HTTP Response Code	Unique Code	Description
202		The requested install or preview task has been started.
404	22603	The requested extension cannot be found.
404	22604	The task status for status_id cannot be found.
409	22612	The supplied extension cannot be installed/previewed because it is already installed
409	22611	The supplied extension cannot be installed/previewed because it is already in the process of being installed/previewed.
409	22618	The requested task can not be initiated because another preview/install task is already in progress.
422	22605	The supplied action type is invalid
422	22606	A supplied numeric parameter was not positive.
500	22602	An error has occurred while trying to install or preview the requested extension.

## Response Description

A JSON string depicting the accepted task for previewing/installing an extension:

- **message** - String - description of the accepted task.
- **status\_location** - String - the url of the task status.
- **current\_status** - String - a JSON object depicting the current status of the task.



## Response Sample

```
{
  "message": "Uninstalling an extension",
  "status_location":
    "https://1.1.1.1/console/restapi/api/config/extension_management/
      extensions_task_status/101",
  "current_status": {
    "progress": 0,
    "result_url": null,
    "cancelled_by": null,
    "status": "QUEUED",
    "task_components": null,
    "modified": 1440891410849,
    "id": 101,
    "message": "Queued Extension uninstallation task for extension id 2",
    "created_by": "admin",
    "created": 1440891410629,
    "maximum": 0,
    "cancel_requested": false,
    "name": "Extension uninstallation task",
    "child_tasks": null,
    "started": 1440891410847,
    "completed": null
  }
}
```

## DELETE /config/extension\_management/extensions/{extension\_id}

Uninstall an extension based on the supplied extension ID. This is an asynchronous action.

Table 134. DELETE /config/extension\_management/extensions/{extension\_id} resource details

MIME Type
application/json

Table 135. DELETE /config/extension\_management/extensions/{extension\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
extension_id	path	Required	Number (Integer)	text/plain	Required - The id of the extension to be uninstalled.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 136. DELETE /config/extension\_management/extensions/{extension\_id} response codes

HTTP Response Code	Unique Code	Description
202		The requested uninstall task has been started.
404	22603	The requested extension cannot be found.
404	22604	The task status for status_id cannot be found.
409	22611	The supplied extension cannot be uninstalled because it is already in the process of being uninstalled.
409	22617	The extension can not be uninstalled because it is already in the process of being previewed/installed.
422	22606	A supplied numeric parameter was not positive.
500	22602	An error has occurred while trying to uninstall an extension.

## Response Description

A JSON string depicting the accepted task for uninstalling an extension:

- **message** - String - description of the accepted task.
- **status\_location** - String - the url of the task status.
- **current\_status** - String - a JSON object depicting the current status of the task.

## Response Sample

```
{
  "message": "Uninstalling an extension",
  "status_location":
    "https://1.1.1.1/console/restapi/api/config/extension_management/
    extensions_task_status/101",
  "current_status": {
    "progress": 0,
    "result_url": null,
    "cancelled_by": null,
    "status": "QUEUED",
    "task_components": null,
    "modified": 1440891410849,
    "id": 101,
    "message": "Queued Extension uninstallation task for extension id 2",
    "created_by": "admin",
    "created": 1440891410629,
    "maximum": 0,
    "cancel_requested": false,
    "name": "Extension uninstallation task",
    "child_tasks": null,
    "started": 1440891410847,
    "completed": null
  }
}
```

## GET /config/extension\_management/extensions\_task\_status/{status\_id}

Retrieves the tasks status based on the status ID.

Table 137. GET /config/extension\_management/extensions\_task\_status/{status\_id} resource details

MIME Type
application/json

Table 138. GET /config/extension\_management/extensions\_task\_status/{status\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
status_id	path	Required	Number (Integer)	text/plain	Required - the id of the task status.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 139. GET /config/extension\_management/extensions\_task\_status/{status\_id} response codes

HTTP Response Code	Unique Code	Description
200		The requested task status has been retrieved.
404	22604	The task status for status_id cannot be found.
422	22606	A supplied numeric parameter was not positive.
500	22602	An error has occurred while trying to retrieve the task status.

### Response Description

A task status containing the following fields:

- **id** - Number - The ID of the task status.
- **name** - String - The name of the task status.
- **status** - String - A string that represents the current state of the task status.
- **message** - String - A message regarding the current state of the task.
- **progress** - Number - The current progress of the task
- **minimum** - Number - The minimum progress of the task.
- **maximum** - Number - The maximum progress of the task.
- **created\_by** - String - The username of the user who created the task.
- **cancelled\_by** - String - The username of the user who cancelled the task.

- **created** - Number - The date/time at which this task was created, represented as number of milliseconds since Unix epoch.
- **started** - Number - The date/time at which this task was started, represented as number of milliseconds since Unix epoch.
- **modified** - Number - The date/time at which this task was last modified, represented as number of milliseconds since Unix epoch.
- **completed** - Number - The date/time at which this task was completed, represented as number of milliseconds since Unix epoch.
- **result\_url** - String - The url where the result can be viewed.
- **cancel\_requested** - Boolean - True if cancel has been requested.
- **child\_tasks** - Array - Array of child task id's that are executed asynchronously from this task.
- **task\_components** - Array - Array of task components that are executed sequentially.

### Response Sample

```
{
  "progress": 0,
  "result_url": "",
  "cancel_requested_by": "",
  "status": "COMPLETED",
  "task_components": null,
  "modified": 1440891517961,
  "id": 102,
  "message": "Completed Extension uninstallation task for extension id 56",
  "created_by": "admin",
  "created": 1440891514006,
  "maximum": 0,
  "cancel_requested": false,
  "name": "Extension uninstallation task",
  "child_tasks": null,
  "started": 1440891514041,
  "completed": 1440891515224
}
```

## GET /config/extension\_management/extensions\_task\_status/{status\_id}/results

Retrieves the tasks status results based on the status ID.

Table 140. GET /config/extension\_management/extensions\_task\_status/{status\_id}/results resource details

<b>MIME Type</b>
application/json

Table 141. GET /config/extension\_management/extensions\_task\_status/{status\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
status_id	path	Required	Number (Integer)	text/plain	Required - The id of the task status.

Table 141. GET /config/extension\_management/extensions\_task\_status/{status\_id}/results request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 142. GET /config/extension\_management/extensions\_task\_status/{status\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The requested results of the task status have been retrieved.
404	22604	The task status for status_id cannot be found.
404	22614	The task results are not available.
422	22606	A supplied numeric parameter was not positive.
500	22602	An error has occurred while trying to retrieve the results of a task status.

## Response Description

A JSON object representing the result of an Extension preview, install or uninstall task. It contains the following fields:

- **id** - Number - The ID of the extension.
- **task\_type** - String - The type of task that was issued against the Extension.
- **content** - Array - An array of JSON objects representing the contents of the extension and what action is associated with each content item for the task that was executed. Each content item contains the following fields:
  - **name** - String - The name of the content item.
  - **content\_type\_id** - Number - The ID of the type of the content item.
  - **content\_type\_name** - String - The name of the type of the content item.
  - **action** - String - The action taken for the content item.

## Response Sample

```
{
  "id": 56,
  "task_type": "UNINSTALL",
  "content": [
    {
      "content_type_id": 3,
      "name": "SYSTEM-1607",
      "action": "SKIP",
      "content_type_name": "custom_rule"
    }
  ],
}
```

```

    {
      "content_type_id": 28,
      "name": "Asset Reconciliation IPv4 Whitelist",
      "action": "SKIP",
      "content_type_name": "reference_data"
    }
  ]
}

```

---

## GUI application framework endpoints

Use the references for REST API V5 GUI application framework endpoints.

### GET /gui\_app\_framework/application\_creation\_task

Retrieve status details.

Retrieve a list of status details of all asynchronous requests to create applications.

Table 143. GET /gui\_app\_framework/application\_creation\_task resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 144. GET /gui\_app\_framework/application\_creation\_task response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of status details.

### Response Description

The details of the requests to create applications.

### Response Sample

```

[
  {
    "application_id": "101",
    "status": "String <one of: CREATING,
              COMPLETED,
              CANCELLED,
              ERROR>",
    "error_messages": [
      {
        "code": "String <one of: ERROR_DB_UNAVAILABLE,
                          ERROR_FRAMEWORK_UNAVAILABLE,
                          ERROR_CREATING_IMAGE,
                          ERROR_STARTING_CONTAINER>",
        "message": "String"
      }
    ]
  }
]

```

## POST /gui\_app\_framework/application\_creation\_task

Create a new application within the Application framework.

Create a new application within the Application framework, and register it with IBM Security QRadar. The application is created asynchronously. A reference to the application\_id is returned and should be used in subsequent API calls to determine the status of the application installation.

Table 145. POST /gui\_app\_framework/application\_creation\_task resource details

MIME Type
application/json

Table 146. POST /gui\_app\_framework/application\_creation\_task request body details

Parameter	Data Type	MIME Type	Description	Sample
package	zip	application/zip	A zip file, that contains custom code, and a application manifest JSON file descriptor	null

Table 147. POST /gui\_app\_framework/application\_creation\_task response codes

HTTP Response Code	Unique Code	Description
201		The application was installed and registered successfully.
422	1005	The provided application is invalid. See messages for further details.
500	1020	The application could not be created.

### Response Description

application id and status

### Response Sample

```
[
  {
    "application_id": "101",
    "status": "String <one of: CREATING,
              COMPLETED,
              CANCELLED,
              ERROR>",
    "error_messages": [
      {
        "code": "String <one of: ERROR_DB_UNAVAILABLE,
                          ERROR_FRAMEWORK_UNAVAILABLE,
                          ERROR_CREATING_IMAGE,
                          ERROR_STARTING_CONTAINER>",
        "message": "String"
      }
    ]
  }
]
```

## GET /gui\_app\_framework/application\_creation\_task/{application\_id}

Retrieve status details.

Retrieve a list of status details of a asynchronous request to create application.

Table 148. GET /gui\_app\_framework/application\_creation\_task/{application\_id} resource details

MIME Type
application/json

Table 149. GET /gui\_app\_framework/application\_creation\_task/{application\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
application_id	path	Required	Number (Integer)	text/plain	Required - Get the status details of this application defined by application_id returned by the initial POST on application_creation_task.

Table 150. GET /gui\_app\_framework/application\_creation\_task/{application\_id} response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
404	1002	The application_id is invalid or could not be found.
500	1020	An error occurred while attempting to retrieve the list of status details.

### Response Description

The details of the request to create application.

### Response Sample

```
[
  {
    "application_id": "101",
    "status": "String <one of: CREATING,
              COMPLETED,
              CANCELLED,
              ERROR>",
    "error_messages": [
      {
        "code": "String <one of: ERROR_DB_UNAVAILABLE,
              ERROR_FRAMEWORK_UNAVAILABLE,
              ERROR_CREATING_IMAGE,
              ERROR_STARTING_CONTAINER>",
        "message": "String"
      }
    ]
  }
]
```



## POST /gui\_app\_framework/application\_creation\_task/{application\_id}

Update a new application install within the Application framework.

Update a new application install within the Application framework The **application\_id** and a **status** are required.

Table 151. POST /gui\_app\_framework/application\_creation\_task/{application\_id} resource details

MIME Type
application/json

Table 152. POST /gui\_app\_framework/application\_creation\_task/{application\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
application_id	path	Required	Number (Integer)	text/plain	Required - The application_id to cancel installing.
status	query	Required	String	text/plain	Required - The status to update the application install to. Currently only CANCELLED is supported

Table 153. POST /gui\_app\_framework/application\_creation\_task/{application\_id} response codes

HTTP Response Code	Unique Code	Description
200		The application was cancelled installing and unregistered successfully.
404	1002	The application_id is invalid or could not be found.
422	1005	The status is not valid.
500	1020	An error occurred when attempting to update the Application request state.

### Response Description

application id and status

### Response Sample

```
[
  {
    "application_id": "101",
    "status": "String <one of: CREATING,
      COMPLETED,
      CANCELLED,
      ERROR>",
    "error_messages": [
      {
        "code": "String <one of: ERROR_DB_UNAVAILABLE,
          ERROR_FRAMEWORK_UNAVAILABLE,
          ERROR_CREATING_IMAGE,
          ERROR_STARTING_CONTAINER>",
        "message": "String"
```

```

    }
  ]
}
]

```

## GET /gui\_app\_framework/applications

Retrieve a list of applications.

Retrieve a list of applications that are installed on the console, with their manifest JSON structures and current status.

Table 154. GET /gui\_app\_framework/applications resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 155. GET /gui\_app\_framework/applications response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of applications.

## Response Description

The list of applications.

## Response Sample

```

[
  {
    "application_state": {
      "application_id": "101",
      "status": "String <one of: CREATING,
                RUNNING,
                STOPPED,
                ERROR>",
      "error_message": "String"
    }
  },
  "manifest": {
    "name": "Sample Application",
    "description": "An example of how to create an application manifest",
    "version": "0.0.1",
    "areas": [
      {
        "id": "Qapp1_HelloWorld",
        "url": "http://9.21.118.58:5000",
        "text": "QApp1",
        "description": "Loading a dockerised web app into a tab
                      inside QRadar",
        "required_capabilities": ["ADMIN"]
      }
    ]
  },
  "dashboard_items": [

```

```

    {
      "text": "Sample Item",
      "description": "Sample dashboard item that is a copy of
                     most recent offenses",
      "rest_method": "sampleDashboardItem",
      "required_capabilities": ["ADMIN"]
    }
  ],
  "rest_methods": [
    {
      "name": "sampleDashboardItem",
      "url": "/static/sampleDashboardItemResponse.json",
      "method": "GET",
      "argument_names": [],
      "required_capabilities": ["ADMIN"]
    },
    {
      "name": "sampleToolBarMethod",
      "url": "/static/sampleToolBarButtonResponse.json",
      "method": "GET",
      "argument_names": ["context"],
      "required_capabilities": ["ADMIN"]
    },
    {
      "name": "sampleIPInformation",
      "url": "/static/sampleIPInformationResponse.json",
      "method": "GET",
      "argument_names": ["metaDataContext"],
      "required_capabilities": ["ADMIN"]
    },
    {
      "name": "sampleUserInformation",
      "url": "/static/sampleUserInformationResponse.json",
      "method": "GET",
      "argument_names": ["metaDataContext"],
      "required_capabilities": ["ADMIN"]
    },
    {
      "name": "sampleURLInformation",
      "url": "/static/sampleURLInformationResponse.json",
      "method": "GET",
      "argument_names": ["metaDataContext"],
      "required_capabilities": ["ADMIN"]
    },
    {
      "name": "addToReferenceSet",
      "url": "/addToReferenceSet",
      "method": "GET",
      "argument_names": ["data"]
    }
  ],
  "configuration_pages": [
    {
      "text": "Open IBM.com",
      "description": "Loading IBM.com in a new window",
      "icon": null,
      "url": "https://www.ibm.com/us/en/",
      "required_capabilities": ["ADMIN"]
    }
  ],
  "gui_actions": [
    {
      "id": "addToReferenceSet",
      "text": "Add To Reference Set",

```

```

        "description":"Adds to a reference set",
        "icon":null,
        "rest_method":"addToReferenceSet",
        "javascript":"alert(result)",
        "groups":[ "ipPopup" ],
        "required_capabilities":[ "ADMIN" ]
    },
    {
        "id":"sampleToolbarButton",
        "text":"Sample Toolbar Button",
        "description":"Sample toolbar button that calls a REST method,
            passing an offense ID along",
        "icon":null,
        "rest_method":"sampleToolbarMethod",
        "javascript":"alert(result)",
        "groups":[ "OffenseListToolbar" ],
        "required_capabilities":[ "ADMIN" ]
    }
],
"page_scripts": [
    {
        "app_name":"SEM",
        "page_id":"OffenseList",
        "scripts":["/static/sampleScriptInclude.js"]
    }
],
"metadata_providers": [
    {
        "rest_method":"sampleIPInformation",
        "metadata_type":"ip"
    },
    {
        "rest_method":"sampleUserInformation",
        "metadata_type":"userName"
    },
    {
        "rest_method":"sampleURLInformation",
        "metadata_type":"ariel:URL"
    }
]
}
]

```

## GET /gui\_app\_framework/applications/{application\_id}

Retrieve specific application.

Retrieve a specific application that is installed on the console with manifest JSON structure and current status.

Table 156. GET /gui\_app\_framework/applications/{application\_id} resource details

MIME Type
application/json

Table 157. GET /gui\_app\_framework/applications/{application\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
application_id	path	Required	Number (Integer)	text/plain	Required - Get specific installed application defined by application_id returned by the initial POST on application_creation_task.

Table 158. GET /gui\_app\_framework/applications/{application\_id} response codes

HTTP Response Code	Unique Code	Description
200		The application was retrieved.
404	1002	The applicationid is invalid or could not be found.
500	1020	An error occurred while attempting to retrieve the application.

## Response Description

The specific application.

## Response Sample

```
[
  {
    "application_state":{
      "application_id":"101",
      "status":"String <one of: CREATING,
                                     RUNNING,
                                     STOPPED,
                                     ERROR>",
      "error_message": "String"
    }
  },
  "manifest":{
    "name":"Sample Application",
    "description":"An example of how to create an application manifest",
    "version":"0.0.1",

    "areas": [
      {
        "id":"Qapp1_HelloWorld",
        "url":"http://9.21.118.58:5000",
        "text":"QApp1",
        "description":"Loading a dockerised web app into a tab
                       inside QRadar",
        "required_capabilities":["ADMIN"]
      }
    ],

    "dashboard_items": [
      {
        "text":"Sample Item",
        "description":"Sample dashboard item that is a copy of
                       most recent offenses",
        "rest_method":"sampleDashboardItem",
        "required_capabilities":["ADMIN"]
      }
    ],

    "rest_methods": [
      {
        "name":"sampleDashboardItem",
        "url":"/static/sampleDashboardItemResponse.json",
        "method":"GET",
        "argument_names":[],
        "required_capabilities":["ADMIN"]
      }
    ]
  }
]
```

```

        "name": "sampleToolBarMethod",
        "url": "/static/sampleToolBarButtonResponse.json",
        "method": "GET",
        "argument_names": ["context"],
        "required_capabilities": ["ADMIN"]
    },
    {
        "name": "sampleIPInformation",
        "url": "/static/sampleIPInformationResponse.json",
        "method": "GET",
        "argument_names": ["metaDataContext"],
        "required_capabilities": ["ADMIN"]
    },
    {
        "name": "sampleUserInformation",
        "url": "/static/sampleUserInformationResponse.json",
        "method": "GET",
        "argument_names": ["metaDataContext"],
        "required_capabilities": ["ADMIN"]
    },
    {
        "name": "sampleURLInformation",
        "url": "/static/sampleURLInformationResponse.json",
        "method": "GET",
        "argument_names": ["metaDataContext"],
        "required_capabilities": ["ADMIN"]
    },
    {
        "name": "addToReferenceSet",
        "url": "/addToReferenceSet",
        "method": "GET",
        "argument_names": ["data"]
    }
],
"configuration_pages": [
    {
        "text": "Open IBM.com",
        "description": "Loading IBM.com in a new window",
        "icon": null,
        "url": "https://www.ibm.com/us/en/",
        "required_capabilities": ["ADMIN"]
    }
],
"gui_actions": [
    {
        "id": "addToReferenceSet",
        "text": "Add To Reference Set",
        "description": "Adds to a reference set",
        "icon": null,
        "rest_method": "addToReferenceSet",
        "javascript": "alert(result)",
        "groups": [ "ipPopup" ],
        "required_capabilities": [ "ADMIN" ]
    },
    {
        "id": "sampleToolBarButton",
        "text": "Sample Toolbar Button",
        "description": "Sample toolbar button that calls a REST method,
            passing an offense ID along",
        "icon": null,
        "rest_method": "sampleToolBarMethod",
        "javascript": "alert(result)",
        "groups": [ "OffenseListToolbar" ],
        "required_capabilities": [ "ADMIN" ]
    }
]

```

```

    ],
    "page_scripts": [
      {
        "app_name": "SEM",
        "page_id": "OffenseList",
        "scripts": ["/static/sampleScriptInclude.js"]
      }
    ],
    "metadata_providers": [
      {
        "rest_method": "sampleIPInformation",
        "metadata_type": "ip"
      },
      {
        "rest_method": "sampleUserInformation",
        "metadata_type": "userName"
      },
      {
        "rest_method": "sampleURLInformation",
        "metadata_type": "ariel:URL"
      }
    ]
  }
]

```

## POST /gui\_app\_framework/applications/{application\_id}

Update an application.

Update an application. Start or stop an application by setting status to RUNNING or STOPPED respectively.

Table 159. POST /gui\_app\_framework/applications/{application\_id} resource details

MIME Type
application/json

Table 160. POST /gui\_app\_framework/applications/{application\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
application_id	path	Required	Number (Integer)	text/plain	Required - The applicationId of the application to update.
status	query	Required	String	text/plain	Required - The status of the application to set to RUNNING or STOPPED.

Table 161. POST /gui\_app\_framework/applications/{application\_id} response codes

HTTP Response Code	Unique Code	Description
200		The application has been successfully updated
404	1002	The applicationId does not exist.
422	1005	The application status is not valid.
500	1020	An error occurred while attempting to update the application.

## Response Description

Application structure including application status.

## Response Sample

```
[
  {
    "application_state":{
      "application_id":"101",
      "status":"String <one of: CREATING,
                                RUNNING,
                                STOPPED,
                                ERROR>",
      "error_message": "String"
    }
  },
  "manifest":{
    "name":"Sample Application",
    "description":"An example of how to create an application manifest",
    "version":"0.0.1",

    "areas": [
      {
        "id":"Qapp1_HelloWorld",
        "url":"http://9.21.118.58:5000",
        "text":"QApp1",
        "description":"Loading a dockerised web app into a tab
                      inside QRadar",
        "required_capabilities":["ADMIN"]
      }
    ],

    "dashboard_items": [
      {
        "text":"Sample Item",
        "description":"Sample dashboard item that is a copy of
                      most recent offenses",
        "rest_method":"sampleDashboardItem",
        "required_capabilities":["ADMIN"]
      }
    ],

    "rest_methods": [
      {
        "name":"sampleDashboardItem",
        "url":"/static/sampleDashboardItemResponse.json",
        "method":"GET",
        "argument_names":[],
        "required_capabilities":["ADMIN"]
      },
      {
        "name":"sampleToolbarMethod",
        "url":"/static/sampleToolbarButtonResponse.json",
        "method":"GET",
        "argument_names":["context"],
        "required_capabilities":["ADMIN"]
      },
      {
        "name":"sampleIPInformation",
        "url":"/static/sampleIPInformationResponse.json",
        "method":"GET",
        "argument_names":["metaDataContext"],
        "required_capabilities":["ADMIN"]
      }
    ],
  }
]
```



```

        "name": "sampleUserInformation",
        "url": "/static/sampleUserInformationResponse.json",
        "method": "GET",
        "argument_names": ["metaDataContext"],
        "required_capabilities": ["ADMIN"]
    },
    {
        "name": "sampleURLInformation",
        "url": "/static/sampleURLInformationResponse.json",
        "method": "GET",
        "argument_names": ["metaDataContext"],
        "required_capabilities": ["ADMIN"]
    },
    {
        "name": "addToReferenceSet",
        "url": "/addToReferenceSet",
        "method": "GET",
        "argument_names": ["data"]
    }
],
"configuration_pages": [
    {
        "text": "Open IBM.com",
        "description": "Loading IBM.com in a new window",
        "icon": null,
        "url": "https://www.ibm.com/us/en/",
        "required_capabilities": ["ADMIN"]
    }
],
"gui_actions": [
    {
        "id": "addToReferenceSet",
        "text": "Add To Reference Set",
        "description": "Adds to a reference set",
        "icon": null,
        "rest_method": "addToReferenceSet",
        "javascript": "alert(result)",
        "groups": [ "ipPopup" ],
        "required_capabilities": [ "ADMIN" ]
    },
    {
        "id": "sampleToolbarButton",
        "text": "Sample Toolbar Button",
        "description": "Sample toolbar button that calls a REST method,
            passing an offense ID along",
        "icon": null,
        "rest_method": "sampleToolbarMethod",
        "javascript": "alert(result)",
        "groups": [ "OffenseListToolbar" ],
        "required_capabilities": [ "ADMIN" ]
    }
],
"page_scripts": [
    {
        "app_name": "SEM",
        "page_id": "OffenseList",
        "scripts": [ "/static/sampleScriptInclude.js" ]
    }
],
"metadata_providers": [
    {
        "rest_method": "sampleIPInformation",
        "metadata_type": "ip"
    }
]

```

```

    },
    {
      "rest_method": "sampleUserInformation",
      "metadata_type": "userName"
    },
    {
      "rest_method": "sampleURLInformation",
      "metadata_type": "ariel:URL"
    }
  ]
}
]

```

## DELETE /gui\_app\_framework/applications/{application\_id}

Delete an application.

Table 162. DELETE /gui\_app\_framework/applications/{application\_id} resource details

MIME Type
text/plain

Table 163. DELETE /gui\_app\_framework/applications/{application\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
application_id	path	Required	Number (Integer)	text/plain	Required - The applicationId of the application to delete.

Table 164. DELETE /gui\_app\_framework/applications/{application\_id} response codes

HTTP Response Code	Unique Code	Description
204		The application has been successfully unregistered.
404	1002	The applicationId does not exist.
500	1020	An error occurred while attempting to delete the application.

### Response Description

Successful response code 204 No content.

### Response Sample

---

## Help endpoints

Use the references for REST API V5 Help endpoints.

### GET /help/capabilities

List all QRadar API capabilities

List the QRadar API capabilities. The response will contain all available RESTful resources We allow every authenticated user to access this method, but restrict the output based on their user capabilities

Table 165. GET /help/capabilities resource details

<b>MIME Type</b>
application/json

Table 166. GET /help/capabilities request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
categories	query	Optional	Array<String>	application/json	Optional - Restrict your search to this list of capabilities
paths	query	Optional	Array<String>	application/json	Optional - Restrict your search to these paths only
httpMethods	query	Optional	Array<String>	application/json	Optional - Restrict your search to these HTTP methods
version	query	Optional	String	text/plain	Optional - Restrict your search to this version (or below)
showExperimental	query	Optional	Boolean	text/plain	Optional - If true, we include experimental endpoints (default is true)
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 167. GET /help/capabilities response codes

HTTP Response Code	Unique Code	Description
200		The API capabilities list was retrieved.
422	1001	Invalid input
422	1002	Our internal mapping has an unexpected structure or contains an invalid element value
500	1003	A generic error has occurred while retrieving our capabilities

## Response Description

Endpoints you are able to access, mapped against versions they belong to. If full content is not requested, values will be null.

## Response Sample

```
{
  "categories": [
    {
      "apis": [
        {
          "httpMethod": "String <one of: OPTIONS,
            GET,
            HEAD,
            POST,
            PUT,
```

```

DELETE,
TRACE,
CONNECT,
PATCH>",
"operations": [
  {
    "additionalFiltering": true,
    "deprecated": true,
    "description": "String",
    "errorResponses": [
      {
        "code": 42,
        "description": "String",
        "uniqueCode": 42
      }
    ],
    "httpMethod": "String",
    "lastSupportedVersion": "String",
    "parameters": [
      {
        "allowMultiple": true,
        "defaultValue": "String",
        "description": "String",
        "name": "String",
        "pathIndex": 42,
        "required": true,
        "source": "String",
        "supportedContentTypes": [
          {
            "dataType": "String",
            "mimeType": "String",
            "sample": "String"
          }
        ]
      }
    ]
  },
  "removalTarget": "String",
  "removed": true,
  "responseClass": "String",
  "responseDescription": {
    "description": "String",
    "properties": [
      {
        "description": "String",
        "name": "String"
      }
    ]
  },
  "successResponses": [
    {
      "code": 42,
      "description": "String"
    }
  ],
  "summary": "String",
  "supportedContentTypes": [
    {
      "dataType": "String",
      "mimeType": "String",
      "sample": "String"
    }
  ],
  "version": "String",
  "visibility": "String"
},
"path": "String"

```

```

    ],
    "path": "String"
  },
  ],
  "path": "String"
}

```

## QRadar Vulnerability Manager endpoints

Use the references for REST API V5 QRadar Vulnerability Manager endpoints.

### GET /qvm/assets

List the assets with discovered vulnerabilities present in the asset model. The response contains all available RESTful resources.

Table 168. GET /qvm/assets resource details

<b>MIME Type</b>
application/json

Table 169. GET /qvm/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 170. GET /qvm/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by asset completed successfully
420	9101	Invalid search parameters, search cannot be performed

### Response Description

list of assets data

### Response Sample

### GET /qvm/filters

Get a list of the allowable filters that can be used or applied against /qvm endpoints.

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices

- /qvm/networks
- queries

Table 171. GET /qvm/filters resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 172. GET /qvm/filters response codes

HTTP Response Code	Unique Code	Description
200		The search executed successfully
420	9102	An error occurred while executing the search

## Response Description

list of Filters.

## Response Sample

## GET /qvm/network

List the networks present in the asset model with vulnerabilities present. The response contains all available RESTful resources

Table 173. GET /qvm/network resource details

<b>MIME Type</b>
application/json

Table 174. GET /qvm/network request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 175. GET /qvm/network response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by network completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of network related data

## Response Sample

### GET /qvm/openservices

List the openservices present in the asset model with vulnerabilities present. The response will contain all available RESTful resources

Table 176. GET /qvm/openservices resource details

MIME Type
application/json

Table 177. GET /qvm/openservices request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 178. GET /qvm/openservices response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by open service completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of open services related data

## Response Sample

### GET /qvm/savedsearches

Get a list of saved searches that can be applied against /qvm endpoints.

A list of saved searches that can be applied against the following endpoints:

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 179. GET /qvm/savedsearches resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 180. GET /qvm/savedsearches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully
420	9103	An error occurred while trying to retrieve the list of saved searches

## Response Description

list of saved searches. Per saved search: id, name and list fo filters that make up this saved search

## Response Sample

## POST /qvm/tickets/assign

Update the remediation ticket for the assigned vulnerability

Table 181. POST /qvm/tickets/assign resource details

<b>MIME Type</b>
application/json

Table 182. POST /qvm/tickets/assign request body details

Parameter	Data Type	MIME Type	Description	Sample
ticket	JSON	application/json	<p>'ticketId': required.</p> <p>'priority' one of required : Critical, Major, Minor, Warning, Informational.</p> <p>'status' one of required : Opened, Fixed, Re-Opened, Closed .</p> <p>'dueDate' Optional : yyyy-MM-dd HH:mm:ss.</p> <p>'assignedUser' required : valid QRadar user account name or a valid email.</p> <p>'comment' Optional : text.</p> <p>'commentUser' Optional : valid QRadar user account name, if not included will default current API user.</p>	[ { "ticketId":"1000", "status":"Opened", "priority":"Critical", "dueDate":"2015-01-04 12:00:00", "assignedUser":"admin", "comment":"testComment", "commentUser":"admin" } ]

Table 183. POST /qvm/tickets/assign response codes

HTTP Response Code	Unique Code	Description
200		The request to assign a ticket completed successfully



Table 183. POST /qvm/tickets/assign response codes (continued)

HTTP Response Code	Unique Code	Description
420	9104	An error occurred while trying to assign a ticket due to invalid arguments

## Response Description

success message if update succeed

## Response Sample

## GET /qvm/vulninstances

List the Vulnerability Instances present in the asset model. The response will contain all available RESTful resources

Table 184. GET /qvm/vulninstances resource details

MIME Type
application/json

Table 185. GET /qvm/vulninstances request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 186. GET /qvm/vulninstances response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by instance completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability instance data

## Response Sample

## GET /qvm/vulns

List the Vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 187. GET /qvm/vulns resource details

<b>MIME Type</b>
application/json

Table 188. GET /qvm/vulns request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 189. GET /qvm/vulns response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability data

## Response Sample

---

## Reference data endpoints

Use the references for REST API V5 reference data endpoints.

### GET /reference\_data/map\_of\_sets

Retrieve a list of all reference map of sets.

Table 190. GET /reference\_data/map\_of\_sets resource details

<b>MIME Type</b>
application/json

Table 191. GET /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 192. GET /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

## Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## POST /reference\_data/map\_of\_sets

Create a new reference map of sets.

Table 193. POST /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 194. POST /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 195. *POST /reference\_data/map\_of\_sets* response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/map\_of\_sets/{name}

Return the reference map of sets identified by name.

Return the reference map of sets identified by **name**. If provided, **limit** specifies the number of records to return starting at the record that is specified by **offset**. If the number is not specified, then the first 20 records is returned.

Table 196. *GET /reference\_data/map\_of\_sets/{name}* resource details

MIME Type
application/json

Table 197. *GET /reference\_data/map\_of\_sets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve

Table 197. GET /reference\_data/map\_of\_sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 198. GET /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map of sets

## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": [
      {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    ]
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
}
```

```

"time_to_live": "String",
"timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"value_label": "String"
}

```

## POST /reference\_data/map\_of\_sets/{name}

Add or update an element in a reference map of sets.

Table 199. POST /reference\_data/map\_of\_sets/{name} resource details

<b>MIME Type</b>
application/json

Table 200. POST /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 201. POST /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid

Table 201. *POST /reference\_data/map\_of\_sets/{name}* response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to add or update data in the reference map of sets

## Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name}

Remove a map of sets or purge its contents.

Table 202. *DELETE /reference\_data/map\_of\_sets/{name}* resource details

MIME Type
application/json

Table 203. *DELETE /reference\_data/map\_of\_sets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.



Table 203. DELETE /reference\_data/map\_of\_sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 204. DELETE /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Map of Sets deletion or purge request has been accepted and is in progress
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

## Response Description

A status\_id to retrieve the Reference Data Map of Sets deletion or purge status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{
  "current_status": {
    "cancel_requested": true,
    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
      CANCELING,
      CANCEL_REQUESTED,
      COMPLETED,
      EXCEPTION,
      INITIALIZING,
```

```

    INTERRUPTED,
    PAUSED,
    PROCESSING,
    QUEUED,
    RESUMING>",
    "task_components": [
      {
        "completed": 42,
        "created": 42,
        "maximum": 42,
        "message": "String",
        "modified": 42,
        "progress": 42,
        "started": 42,
        "status": "String <one of: CANCELLED,
        CANCELING,
        CANCEL_REQUESTED,
        COMPLETED,
        EXCEPTION,
        INITIALIZING,
        INTERRUPTED,
        PAUSED,
        PROCESSING,
        QUEUED,
        RESUMING>"
      }
    ]
  },
  "message": "String",
  "status_location": "String"
}

```

## GET /reference\_data/map\_of\_sets/{name}/dependents

Retrieves the dependents of the Map of Sets.

Initiates the retrieval of dependents of the Map of Sets

Table 205. GET /reference\_data/map\_of\_sets/{name}/dependents resource details

MIME Type
application/json

Table 206. GET /reference\_data/map\_of\_sets/{name}/dependents request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets retrieve dependents for
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 207. GET /reference\_data/map\_of\_sets/{name}/dependents response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Map of Sets dependent retrieval request has been accepted and is in progress
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to get the dependents for the reference map of sets

## Response Description

A status\_id to retrieve the Reference Data Map of Sets dependent retrieval status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{
  "current_status": {
    "cancel_requested": true,
    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
      CANCELING,
      CANCEL_REQUESTED,
      COMPLETED,
      EXCEPTION,
      INITIALIZING,
      INTERRUPTED,
      PAUSED,
      PROCESSING,
      QUEUED,
      RESUMING>",
  }
  "task_components": [
    {
      "completed": 42,
      "created": 42,
      "maximum": 42,
      "message": "String",
      "modified": 42,
      "progress": 42,
      "started": 42,
      "status": "String <one of: CANCELLED,
        CANCELING,
        CANCEL_REQUESTED,
        COMPLETED,
        EXCEPTION,
        INITIALIZING,
```

```

    INTERRUPTED,
    PAUSED,
    PROCESSING,
    QUEUED,
    RESUMING>"
  }
}
},
"message": "String",
"status_location": "String"
}

```

## DELETE /reference\_data/map\_of\_sets/{name}/value/{key}

Remove a value from a reference map of sets.

Table 208. DELETE /reference\_data/map\_of\_sets/{name}/value/{key} resource details

MIME Type
application/json

Table 209. DELETE /reference\_data/map\_of\_sets/{name}/value/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 210. DELETE /reference\_data/map\_of\_sets/{name}/value/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist

Table 210. DELETE /reference\_data/map\_of\_sets/{name}/value/{key} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

## Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps

Retrieve a list of all reference maps.

Table 211. GET /reference\_data/maps resource details

MIME Type
application/json

Table 212. GET /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 212. GET /reference\_data/maps request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 213. GET /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

## Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## POST /reference\_data/maps

Create a new reference map.

Table 214. POST /reference\_data/maps resource details

MIME Type
application/json

Table 215. POST /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 216. POST /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid

Table 216. *POST /reference\_data/maps* response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps/{name}

Retrieve the reference map identified by name.

Retrieve the reference map identified by **name**. If it is provided, **limit** specifies the number of records to return starting at record that is specified by **offset**. If the number is not specified, then the first 20 records are returned.

Table 217. *GET /reference\_data/maps/{name}* resource details

MIME Type
application/json

Table 218. *GET /reference\_data/maps/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.



Table 218. GET /reference\_data/maps/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 219. GET /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/maps/{name}

Add or update an element in a reference map.

Table 220. POST /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 221. POST /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 222. POST /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/maps/{name}

Remove a reference map or purge its contents.

Table 223. DELETE /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 224. DELETE /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 225. DELETE /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Maps deletion or purge request has been accepted and is in progress
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

## Response Description

A status\_id to retrieve the Reference Data Maps deletion or purge status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{
  "current_status": {
    "cancel_requested": true,
    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
      CANCELING,
      CANCEL_REQUESTED,
      COMPLETED,
      EXCEPTION,
      INITIALIZING,
      INTERRUPTED,
      PAUSED,
      PROCESSING,
      QUEUED,
      RESUMING>",
  }
  "task_components": [
    {
      "completed": 42,
      "created": 42,
      "maximum": 42,
      "message": "String",
      "modified": 42,
      "progress": 42,
      "started": 42,
      "status": "String <one of: CANCELLED,
        CANCELING,
        CANCEL_REQUESTED,
        COMPLETED,
        EXCEPTION,
        INITIALIZING,
```

```

    INTERRUPTED,
    PAUSED,
    PROCESSING,
    QUEUED,
    RESUMING>"
  }
]
},
"message": "String",
"status_location": "String"
}

```

## GET /reference\_data/maps/{name}/dependents

Retrieves the dependents of the Map.

Table 226. GET /reference\_data/maps/{name}/dependents resource details

<b>MIME Type</b>
application/json

Table 227. GET /reference\_data/maps/{name}/dependents request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map retrieve dependents for
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 228. GET /reference\_data/maps/{name}/dependents response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Maps dependent retrieval request has been accepted and is in progress
404	1002	The reference Map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to get the dependents for the reference map

## Response Description

A status\_id to retrieve the Reference Data Maps dependent retrieval status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{
  "current_status": {
    "cancel_requested": true,
    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
              CANCELING,
              CANCEL_REQUESTED,
              COMPLETED,
              EXCEPTION,
              INITIALIZING,
              INTERRUPTED,
              PAUSED,
              PROCESSING,
              QUEUED,
              RESUMING>"
  },
  "task_components": [
    {
      "completed": 42,
      "created": 42,
      "maximum": 42,
      "message": "String",
      "modified": 42,
      "progress": 42,
      "started": 42,
      "status": "String <one of: CANCELLED,
                CANCELING,
                CANCEL_REQUESTED,
                COMPLETED,
                EXCEPTION,
                INITIALIZING,
                INTERRUPTED,
                PAUSED,
                PROCESSING,
                QUEUED,
                RESUMING>"
    }
  ],
  "message": "String",
  "status_location": "String"
}
```

## DELETE /reference\_data/maps/{name}/value/{key}

Remove a value from a reference map.

Table 229. DELETE /reference\_data/maps/{name}/value/{key} resource details

MIME Type
application/json

Table 230. DELETE /reference\_data/maps/{name}/value/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 231. DELETE /reference\_data/maps/{name}/value/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

## Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/sets

Retrieve a list of all reference sets.

Table 232. GET /reference\_data/sets resource details

<b>MIME Type</b>
application/json

Table 233. GET /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 234. GET /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

### Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

### Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "number_of_elements": 42,
```



```

    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]

```

## POST /reference\_data/sets

Create a new reference set.

Table 235. POST /reference\_data/sets resource details

MIME Type
application/json

Table 236. POST /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 237. POST /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/sets/{name}

Retrieve the reference set identified by name.

Retrieve the reference set that is identified by **name**. If it is provided, **limit** specifies the number of records to return starting at the record that is specified by **offset**. If the number is not specified, then the first 20 records are returned.

Table 238. GET /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 239. GET /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 239. GET /reference\_data/sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 240. GET /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": [
    {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  ],
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/{name}

Add or update an element in a reference set.

Table 241. POST /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 242. POST /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 243. POST /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update an element in the reference set

### Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/sets/{name}

Remove a reference set or purge its contents.

Table 244. DELETE /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 245. DELETE /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 246. DELETE /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Sets deletion or purge request has been accepted and is in progress
404	1002	The reference set does not exist

Table 246. DELETE /reference\_data/sets/{name} response codes (continued)

HTTP Response Code	Unique Code	Description
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference set

## Response Description

A status\_id to retrieve the Reference Data Sets deletion or purge status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{
  "current_status": {
    "cancel_requested": true,
    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
      CANCELING,
      CANCEL_REQUESTED,
      COMPLETED,
      EXCEPTION,
      INITIALIZING,
      INTERRUPTED,
      PAUSED,
      PROCESSING,
      QUEUED,
      RESUMING>",
  },
  "task_components": [
    {
      "completed": 42,
      "created": 42,
      "maximum": 42,
      "message": "String",
      "modified": 42,
      "progress": 42,
      "started": 42,
      "status": "String <one of: CANCELLED,
        CANCELING,
        CANCEL_REQUESTED,
        COMPLETED,
        EXCEPTION,
        INITIALIZING,
        INTERRUPTED,
        PAUSED,
        PROCESSING,
        QUEUED,
        RESUMING>",
    }
  ]
}
```

RESUMING>"

```
    }  
  ],  
  },  
  "message": "String",  
  "status_location": "String"  
}
```

## GET /reference\_data/sets/{name}/dependents

Retrieves the dependents of the set.

Table 247. GET /reference\_data/sets/{name}/dependents resource details

<b>MIME Type</b>
application/json

Table 248. GET /reference\_data/sets/{name}/dependents request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the Reference Set retrieve dependents for
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 249. GET /reference\_data/sets/{name}/dependents response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Sets dependent retrieval request has been accepted and is in progress
404	1002	The Reference Set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to get the dependents for the Reference Set

## Response Description

A status\_id to retrieve the Reference Data Sets dependent retrieval status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{  
  "current_status": {  
    "cancel_requested": true,  
  }  
}
```

```

    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
      CANCELING,
      CANCEL_REQUESTED,
      COMPLETED,
      EXCEPTION,
      INITIALIZING,
      INTERRUPTED,
      PAUSED,
      PROCESSING,
      QUEUED,
      RESUMING>",
    "task_components": [
      {
        "completed": 42,
        "created": 42,
        "maximum": 42,
        "message": "String",
        "modified": 42,
        "progress": 42,
        "started": 42,
        "status": "String <one of: CANCELLED,
          CANCELING,
          CANCEL_REQUESTED,
          COMPLETED,
          EXCEPTION,
          INITIALIZING,
          INTERRUPTED,
          PAUSED,
          PROCESSING,
          QUEUED,
          RESUMING>"
      }
    ]
  },
  "message": "String",
  "status_location": "String"
}

```

## DELETE /reference\_data/sets/{name}/value/{value}

Remove a value from a reference set.

Table 250. DELETE /reference\_data/sets/{name}/value/{value} resource details

MIME Type
application/json



Table 251. DELETE /reference\_data/sets/{name}/value/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 252. DELETE /reference\_data/sets/{name}/value/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had an value removed. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/bulk\_load/{name}

Add or update data in a reference set.

Table 253. POST /reference\_data/sets/bulk\_load/{name} resource details

MIME Type
application/json

Table 254. POST /reference\_data/sets/bulk\_load/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 255. POST /reference\_data/sets/bulk\_load/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Array	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 256. POST /reference\_data/sets/bulk\_load/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

### Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables

Retrieve a list of all reference tables.

Table 257. GET /reference\_data/tables resource details

MIME Type
application/json

Table 258. GET /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 259. GET /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "key_name_types": {
      "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    },
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## POST /reference\_data/tables

Create a new reference table.

Table 260. POST /reference\_data/tables resource details

<b>MIME Type</b>
application/json

Table 261. POST /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create
element_type	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>key_name_types</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outer_key_label	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 261. *POST /reference\_data/tables* request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
key_name_types	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 262. *POST /reference\_data/tables* response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables/{name}

Return the reference table identified by name.

Return the reference table that is identified by **name**. If it is provided, **limit** specifies the number of records to return starting at the record that is specified by **offset**. If the number is not specified, then the first 20 records are returned.

Table 263. *GET /reference\_data/tables/{name}* resource details

MIME Type
application/json

Table 264. GET /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 265. GET /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "String": {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
}
```

```

    "key_name_types": {
      "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    },
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }

```

## POST /reference\_data/tables/{name}

Add or update an element in a reference table.

Add or update an element in a reference table. The value to be added must be of the appropriate type. Either the type that corresponds to the **innerKey** that is predefined for the reference table, or the default **elementType** of the reference table

Table 266. POST /reference\_data/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 267. POST /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to add or update an element in
outer_key	query	Required	String	text/plain	Required - The outer key for the element to add or update
inner_key	query	Required	String	text/plain	Required - The inner key for the element to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 267. *POST /reference\_data/tables/{name}* request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 268. *POST /reference\_data/tables/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table

## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/tables/{name}

Remove a reference table or purge its contents.

Table 269. *DELETE /reference\_data/tables/{name}* resource details

MIME Type
application/json



Table 270. DELETE /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 271. DELETE /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Tables deletion or purge request has been accepted and is in progress
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

## Response Description

A status\_id to retrieve the Reference Data Tables deletion or purge status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{
  "current_status": {
    "cancel_requested": true,
    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
  },
}
```

```

    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
                CANCELING,
                CANCEL_REQUESTED,
                COMPLETED,
                EXCEPTION,
                INITIALIZING,
                INTERRUPTED,
                PAUSED,
                PROCESSING,
                QUEUED,
                RESUMING>",
    "task_components": [
        {
            "completed": 42,
            "created": 42,
            "maximum": 42,
            "message": "String",
            "modified": 42,
            "progress": 42,
            "started": 42,
            "status": "String <one of: CANCELLED,
                CANCELING,
                CANCEL_REQUESTED,
                COMPLETED,
                EXCEPTION,
                INITIALIZING,
                INTERRUPTED,
                PAUSED,
                PROCESSING,
                QUEUED,
                RESUMING>"
        }
    ],
    "message": "String",
    "status_location": "String"
}

```

## GET /reference\_data/tables/{name}/dependents

Retrieves the dependents of the Table.

Table 272. GET /reference\_data/tables/{name}/dependents resource details

MIME Type
application/json

Table 273. GET /reference\_data/tables/{name}/dependents request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets retrieve dependents for
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 274. GET /reference\_data/tables/{name}/dependents response codes

HTTP Response Code	Unique Code	Description
202		The Reference Data Tables dependent retrieval request has been accepted and is in progress
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to get the dependents for the reference map of sets

## Response Description

A status\_id to retrieve the Reference Data Tables dependent retrieval status with at /api/system/task\_management/task/{status\_id}. You can also find the url in the Location header

## Response Sample

```
{
  "current_status": {
    "cancel_requested": true,
    "cancelled_by": "String",
    "child_tasks": [
      42
    ],
    "completed": 42,
    "created": 42,
    "created_by": "String",
    "id": 42,
    "maximum": 42,
    "message": "String",
    "modified": 42,
    "name": "String",
    "progress": 42,
    "result_url": "String",
    "started": 42,
    "status": "String <one of: CANCELLED,
      CANCELING,
```

```

    CANCEL_REQUESTED,
    COMPLETED,
    EXCEPTION,
    INITIALIZING,
    INTERRUPTED,
    PAUSED,
    PROCESSING,
    QUEUED,
    RESUMING>",
    "task_components": [
      {
        "completed": 42,
        "created": 42,
        "maximum": 42,
        "message": "String",
        "modified": 42,
        "progress": 42,
        "started": 42,
        "status": "String <one of: CANCELLED,
        CANCELING,
        CANCEL_REQUESTED,
        COMPLETED,
        EXCEPTION,
        INITIALIZING,
        INTERRUPTED,
        PAUSED,
        PROCESSING,
        QUEUED,
        RESUMING>"
      }
    ],
    "message": "String",
    "status_location": "String"
  }
}

```

## DELETE /reference\_data/tables/{name}/value/{outer\_key}/{inner\_key}

Remove a value from a reference table.

Table 275. DELETE /reference\_data/tables/{name}/value/{outer\_key}/{inner\_key} resource details

MIME Type
application/json

Table 276. DELETE /reference\_data/tables/{name}/value/{outer\_key}/{inner\_key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from
outer_key	path	Required	String	text/plain	Required - The outer key of the value to remove
inner_key	path	Required	String	text/plain	Required - The inner key of the value to remove

Table 276. DELETE /reference\_data/tables/{name}/value/{outer\_key}/{inner\_key} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 277. DELETE /reference\_data/tables/{name}/value/{outer\_key}/{inner\_key} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference table value

## Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## Scanner endpoints

Use the references for REST API V5 scanner endpoints.

### GET /scanner/profiles

Retrieves all of the currently created scan profiles.

No parameters are required and the following information should be retrieved for each scan profile.

- **scanProfileId**
- **scanProfileName**
- **description**
- **scanType**
- **scannerName**

Table 278. GET /scanner/profiles resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 279. GET /scanner/profiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

### Response Description

The list of scan profiles currently configured in QVM

### Response Sample

### POST /scanner/profiles/create

Initiates a request to create a new Scan Profile.

The request takes one parameter - **createScanRequest**, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and IP addresses to scan. For example:

```
{'name':'New Scan Profile', 'ips':['10.100.85.135']}
```

Table 280. POST /scanner/profiles/create resource details

MIME Type
text/plain

Table 281. POST /scanner/profiles/create request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 282. POST /scanner/profiles/create response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
419	9101	Occurs when a parameter is missing or invalid
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been created successfully or not.

## Response Sample

String

## POST /scanner/profiles/start

Initiates a request to start an already created scanProfile.

The request takes one parameter - **scanProfileId**. To get a list of scanProfileIds, get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The scanProfileId is validated and an appropriate message is returned.

Table 283. POST /scanner/profiles/start resource details

MIME Type
text/plain

Table 284. POST /scanner/profiles/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
scanProfileId	query	Required	String	text/plain	The unique id of the scan profile we want to start

Table 285. POST /scanner/profiles/start response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles

Retrieves all of the currently created scan profiles.

No parameters are required and the following information should be retrieved for each scan profile.

- **scanProfileId**
- **scanProfileName**
- **description**
- **scanType**
- **scannerName**
- **schedule**
- **status**
- **progress**
- **endTime**
- **duration**

Table 286. GET /scanner/scanprofiles resource details

<b>MIME Type</b>
application/json

Table 287. GET /scanner/scanprofiles request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.



Table 288. GET /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
  }
]
```

## POST /scanner/scanprofiles

Initiates a request to create a new scanProfile.

The request takes one parameter - **createScanRequest**, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and hosts to scan. For example:

```
{'name':'New Scan Profile', 'hosts':['10.100.85.135']}
```

Table 289. POST /scanner/scanprofiles resource details

MIME Type
text/plain

Table 290. POST /scanner/scanprofiles request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	Object	application/json	null	{ "description": "String", "hosts": [ "String" ], "name": "String" }

Table 291. POST /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been created successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles/{profileid}

Retrieves a scan profile for a given Scan Profile ID.

No parameters are required and the following information should be retrieved for each scan profile.

- **scanProfileId**
- **name**
- **description**
- **scanType**
- **scannerName**
- **schedule**
- **status**
- **progress**
- **endTime**
- **duration**

Table 292. GET /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 293. GET /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we need to retrieve information for

Table 293. GET /scanner/scanprofiles/{profileid} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 294. GET /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
200		The scan profile was successfully returned
500	1030	Occurs when an attempt is made to list a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
```

```

        "hours": 42,
        "minutes": 42,
        "month": 42,
        "seconds": 42,
        "time": 42,
        "timezoneOffset": 42,
        "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
}
]

```

## POST /scanner/scanprofiles/{profileid}

Update a scan profile. The Scan Profile ID is required.

The following information on a scan profile can be updated:

- name
- description
- IP addresses

For example:

```
{'name':'Updated Scan Profile', 'ips':['10.100.85.135']}
```

Table 295. POST /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 296. POST /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile used to update

Table 297. POST /scanner/scanprofiles/{profileid} request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 298. POST /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
202		The scan profile was successfully updated
500	1030	Occurs when an attempt is made to update a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

A message to indicate whether the scan profile has updated or not.

## Response Sample

### DELETE /scanner/scanprofiles/{profileid}

Initiates a request to delete a scanProfile.

The request takes one parameter - the Scan Profile ID.

Table 299. DELETE /scanner/scanprofiles/{profileid} resource details

MIME Type
text/plain

Table 300. DELETE /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	null

Table 301. DELETE /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
204		The scan has been successfully deleted
500	1030	Occurs when an attempt is made to delete a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been deleted successfully or not.

## Response Sample

String

### POST /scanner/scanprofiles/{profileid}/start

Initiates a request to start an already created scanProfile.

The request takes one parameter, **scanProfileId**, and one optional parameter, **ips**. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The **scanProfileId**, is validated and an appropriate message returned.

Table 302. POST /scanner/scanprofiles/{profileid}/start resource details

MIME Type
text/plain

Table 303. POST /scanner/scanprofiles/{profileid}/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we want to start

Table 304. POST /scanner/scanprofiles/{profileid}/start request body details

Parameter	Data Type	MIME Type	Description	Sample
ips	JSON	application/json	null	null

Table 305. POST /scanner/scanprofiles/{profileid}/start response codes

HTTP Response Code	Unique Code	Description
202		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

---

## SIEM endpoints

Use the references for REST API V5 SIEM endpoints.

### GET /siem/local\_destination\_addresses

Retrieve a list offense local destination addresses currently in the system.

Table 306. GET /siem/local\_destination\_addresses resource details

MIME Type
application/json

Table 307. GET /siem/local\_destination\_addresses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 308. GET /siem/local\_destination\_addresses response codes

HTTP Response Code	Unique Code	Description
200		The local destination address list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the local destination address list was being retrieved.

## Response Description

An array of local destination address objects. A local destination address object contains the following fields:

- **id** - Number - The ID of the destination address.
- **local\_destination\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the destination address.
- **network** - String - The network of the destination address.
- **offense\_ids** - Array of Numbers - List of offense IDs the destination address is part of.
- **source\_address\_ids** - Array of Numbers - List of source address IDs associated with the destination address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the destination address.

- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
[
  {
    "domain_id": 42,
    "event_flow_count": 42,
    "first_event_flow_seen": 42,
    "id": 42,
    "last_event_flow_seen": 42,
    "local_destination_ip": "String",
    "magnitude": 42,
    "network": "String",
    "offense_ids": [
      42
    ],
    "source_address_ids": [
      42
    ]
  }
]
```

## GET /siem/local\_destination\_addresses/{local\_destination\_address\_id}

Retrieve an offense local destination address.

Table 309. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} resource details

MIME Type
application/json

Table 310. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
local_destination_address_id	path	Required	Number (Integer)	text/plain	Required - The ID of the local destination address to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 311. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} response codes

HTTP Response Code	Unique Code	Description
200		The local destination was retrieved.



Table 311. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1002	No local destination address was found for the provided local_destination_address_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the local destination address was being retrieved.

## Response Description

A local destination address object. A local destination address object contains the following fields:

- **id** - Number - The ID of the destination address.
- **local\_destination\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the destination address.
- **network** - String - The network of the destination address.
- **offense\_ids** - Array of Numbers - List of offense IDs the destination address is part of.
- **source\_address\_ids** - Array of Numbers - List of source address IDs associated with the destination address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the destination address.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
{
  "domain_id": 42,
  "event_flow_count": 42,
  "first_event_flow_seen": 42,
  "id": 42,
  "last_event_flow_seen": 42,
  "local_destination_ip": "String",
  "magnitude": 42,
  "network": "String",
  "offense_ids": [
    42
  ],
  "source_address_ids": [
    42
  ]
}
```

## GET /siem/offense\_closing\_reasons

Retrieve a list of all offense closing reasons.

Table 312. GET /siem/offense\_closing\_reasons resource details

<b>MIME Type</b>
application/json

Table 313. GET /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
include_reserved	query	Optional	Boolean	text/plain	Optional - If true, reserved closing reasons are included in the response. Defaults to false. Reserved closing reasons cannot be used to close an offense.
include_deleted	query	Optional	Boolean	text/plain	Optional - If true, deleted closing reasons are included in the response. Defaults to false. Deleted closing reasons cannot be used to close an offense.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 314. GET /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
200		The closing reasons list was retrieved.
500	1020	An error occurred while the closing reasons list was being retrieved.

## Response Description

An array of ClosingReason objects. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

## Response Sample

```
[
  {
    "id": 42,
    "is_deleted": true,
    "is_reserved": true,
    "text": "String"
  }
]
```

## POST /siem/offense\_closing\_reasons

Create an offense closing reason.

Table 315. POST /siem/offense\_closing\_reasons resource details

MIME Type
application/json

Table 316. POST /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
reason	query	Required	String	text/plain	Required - The text of the offense closing reason must be 5 - 60 characters in length.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 317. POST /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
201		The closing reason was created.
409	1004	The closing reason already exists.
422	1005	A request parameter is not valid.

Table 317. POST /siem/offense\_closing\_reasons response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to create the closing reason.

## Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

## Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

## GET /siem/offense\_closing\_reasons/{closing\_reason\_id}

Retrieve an offense closing reason.

Table 318. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} resource details

MIME Type
application/json

Table 319. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
closing_reason_id	path	Required	Number (Integer)	text/plain	Required - The closing reason ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 320. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} response codes

HTTP Response Code	Unique Code	Description
200		The closing reason was retrieved.

Table 320. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1002	No closing reason was found for the provided closing_reason_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the closing reason.

## Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

## Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

## GET /siem/offenses

Retrieve a list of offenses currently in the system.

Table 321. GET /siem/offenses resource details

MIME Type
application/json

Table 322. GET /siem/offenses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 322. GET /siem/offenses request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 323. GET /siem/offenses response codes

HTTP Response Code	Unique Code	Description
200		The offense list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the offense list was being retrieved.

## Response Description

An array of Offense objects. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense. Filtering is not supported on this field.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.

- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense. Filtering is not supported on this field.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense. Filtering is not supported on this field.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED". The following operators are not supported when you filter on this field: "<", ">", "<=", ">=", "BETWEEN".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers - The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 324. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source

Table 324. Offense Type Codes (continued)

Code	Offense Type
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
[{"credibility": 42,
  "source_address_ids": [42],
  "remote_destination_count": 42,
  "local_destination_address_ids": [42],
  "assigned_to": "String",
  "local_destination_count": 42,
  "source_count": 42,
  "start_time": 42,
  "id": 42,
  "destination_networks": ["String"],
  "inactive": true,
  "protected": true,
  "policy_category_count": 42,
  "description": "String",
  "category_count": 42,
  "domain_id": 42,
  "relevance": 42,
  "device_count": 42,
  "security_category_count": 42,
  "flow_count": 42, "event_count": 42,
  "offense_source": "String",
  "status": "String <one of: OPEN, HIDDEN, CLOSED>",
  "magnitude": 42,
  "severity": 42,
  "username_count": 42,
  "closing_user": "String",
  "follow_up": true,
  "closing_reason_id": 42,
  "close_time": 42,
  "source_network": "String",
  "last_updated_time": 42,
  "categories": ["String"],
  "offense_type": 42}]
```

## GET /siem/offenses/{offense\_id}

Retrieve an offense structure that describes properties of an offense

Table 325. GET /siem/offenses/{offense\_id} resource details

<b>MIME Type</b>
application/json



Table 326. GET /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 327. GET /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense was being retrieved.

## Response Description

An Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.

- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers - The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 328. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port

Table 328. Offense Type Codes (continued)

Code	Offense Type
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
  "close_time": 42,
  "closing_reason_id": 42,
  "closing_user": "String",
  "credibility": 42,
  "description": "String",
  "destination_networks": [
    "String"
  ],
  "device_count": 42,
  "domain_id": 42,
  "event_count": 42,
  "flow_count": 42,
  "follow_up": true,
  "id": 42,
  "inactive": true,
  "last_updated_time": 42,
  "local_destination_address_ids": [
    42
  ],
  "local_destination_count": 42,
  "magnitude": 42,
  "offense_source": "String",
  "offense_type": 42,
  "policy_category_count": 42,
  "protected": true,
  "relevance": 42,
  "remote_destination_count": 42,
  "security_category_count": 42,
  "severity": 42,
  "source_address_ids": [
    42
  ],
  "source_count": 42,
  "source_network": "String",
  "start_time": 42,
  "status": "String <one of: OPEN, HIDDEN, CLOSED>",
  "username_count": 42
}
```

## POST /siem/offenses/{offense\_id}

Update an offense.

Table 329. POST /siem/offenses/{offense\_id} resource details

MIME Type
application/json

Table 330. POST /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The ID of the offense to update.
protected	query	Optional	Boolean	text/plain	Optional - Set to true to protect the offense.
follow_up	query	Optional	Boolean	text/plain	Optional - Set to true to set the follow up flag on the offense.
status	query	Optional	String	text/plain	Optional - The new status for the offense. Set to one of: OPEN, HIDDEN, CLOSED. When the status of an offense is being set to CLOSED, a valid closing_reason_id must be provided. To hide an offense, use the HIDDEN status. To show a previously hidden offense, use the OPEN status.
closing_reason_id	query	Optional	Number (Integer)	text/plain	Optional - The ID of a closing reason. You must provide a valid closing_reason_id when you close an offense.
assigned_to	query	Optional	String	text/plain	Optional - A user to assign the offense to.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 331. POST /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was updated.
403	1009	User does not have the required capability to assign an offense.
404	1002	No offense was found for the provided offense_id.

Table 331. POST /siem/offenses/{offense\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
409	1008	Request cannot be completed due to the state of the offense.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense was being updated.

## Response Description

An updated Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.

- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers -The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 332. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
  "close_time": 42,
  "closing_reason_id": 42,
```

```

    "closing_user": "String",
    "credibility": 42,
    "description": "String",
    "destination_networks": [
      "String"
    ],
    "device_count": 42,
    "domain_id": 42,
    "event_count": 42,
    "flow_count": 42,
    "follow_up": true,
    "id": 42,
    "inactive": true,
    "last_updated_time": 42,
    "local_destination_address_ids": [
      42
    ],
    "local_destination_count": 42,
    "magnitude": 42,
    "offense_source": "String",
    "offense_type": 42,
    "policy_category_count": 42,
    "protected": true,
    "relevance": 42,
    "remote_destination_count": 42,
    "security_category_count": 42,
    "severity": 42,
    "source_address_ids": [
      42
    ],
    "source_count": 42,
    "source_network": "String",
    "start_time": 42,
    "status": "String <one of: OPEN, HIDDEN, CLOSED>",
    "username_count": 42
  }
}

```

## GET /siem/offenses/{offense\_id}/notes

Retrieve a list of notes for an offense.

Table 333. GET /siem/offenses/{offense\_id}/notes resource details

<b>MIME Type</b>
application/json

Table 334. GET /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the notes for.

Table 334. GET /siem/offenses/{offense\_id}/notes request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 335. GET /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
200		The note list was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the note list was being retrieved.

## Response Description

An array of Note objects. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
[
  {
    "create_time": 42,
    "id": 42,
```



```

    "note_text": "String",
    "username": "String"
  }
]

```

## POST /siem/offenses/{offense\_id}/notes

Create a note on an offense.

Table 336. POST /siem/offenses/{offense\_id}/notes resource details

MIME Type
application/json

Table 337. POST /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to add the note to.
note_text	query	Required	String	text/plain	Required - The note text.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 338. POST /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
201		The note was created.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create the note.

## Response Description

The Note object that was created. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## GET /siem/offenses/{offense\_id}/notes/{note\_id}

Retrieve a note for an offense.

Table 339. GET /siem/offenses/{offense\_id}/notes/{note\_id} resource details

MIME Type
application/json

Table 340. GET /siem/offenses/{offense\_id}/notes/{note\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the note from.
note_id	path	Required	Number (Integer)	text/plain	Required - The note ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 341. GET /siem/offenses/{offense\_id}/notes/{note\_id} response codes

HTTP Response Code	Unique Code	Description
200		The note was retrieved.
404	1002	No offense was found for the provided offense_id.
404	1003	No note was found for the provided note_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the note.

## Response Description

The Note object for the note ID. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.

- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

### Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## GET /siem/source\_addresses

Retrieve a list offense source addresses currently in the system.

Table 342. GET /siem/source\_addresses resource details

<b>MIME Type</b>
application/json

Table 343. GET /siem/source\_addresses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 344. GET /siem/source\_addresses response codes

HTTP Response Code	Unique Code	Description
200		The source address list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.

Table 344. GET /siem/source\_addresses response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while the source address list was being retrieved.

## Response Description

An array of source address objects. A source address object contains the following fields:

- **id** - Number - The ID of the source.
- **source\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the source address.
- **network** - String - The network of the source address.
- **offense\_ids** - Array of Numbers - List of offense IDs the source is part of.
- **local\_destination\_address\_ids** - Array of Numbers - List of local destination address IDs associated with the source address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the source.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
[
  {
    "domain_id": 42,
    "event_flow_count": 42,
    "first_event_flow_seen": 42,
    "id": 42,
    "last_event_flow_seen": 42,
    "local_destination_address_ids": [
      42
    ],
    "magnitude": 42,
    "network": "String",
    "offense_ids": [
      42
    ],
    "source_ip": "String"
  }
]
```

## GET /siem/source\_addresses/{source\_address\_id}

Retrieve an offense source address.

Table 345. GET /siem/source\_addresses/{source\_address\_id} resource details

MIME Type
application/json

Table 346. GET /siem/source\_addresses/{source\_address\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
source_address_id	path	Required	Number (Integer)	text/plain	Required - The ID of the source address to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 347. GET /siem/source\_addresses/{source\_address\_id} response codes

HTTP Response Code	Unique Code	Description
200		The source address was retrieved.
404	1002	No source address was found for the provided source_address_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the source address was being retrieved.

## Response Description

A source address object. A source address object contains the following fields:

- **id** - Number - The ID of the source.
- **source\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the source address.
- **network** - String - The network of the source address.
- **offense\_ids** - Array of Numbers - List of offense IDs the source is part of.
- **local\_destination\_address\_ids** - Array of Numbers - List of local destination address IDs associated with the source address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the source.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
{
  "domain_id": 42,
  "event_flow_count": 42,
  "first_event_flow_seen": 42,
  "id": 42,
  "last_event_flow_seen": 42,
  "local_destination_address_ids": [
```

```

    42
  ],
  "magnitude": 42,
  "network": "String",
  "offense_ids": [
    42
  ],
  "source_ip": "String"
}

```

## System endpoints

Use the references for REST API V5 system endpoints.

### GET /system/servers

Retrieve a list of all server hosts in the deployment.

Table 348. GET /system/servers resource details

MIME Type
application/json

Table 349. GET /system/servers request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 350. GET /system/servers response codes

HTTP Response Code	Unique Code	Description
200		The requested list of server records has been successfully retrieved.

Table 350. GET /system/servers response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error has occurred while trying to retrieve the requested servers.

## Response Description

A list of the servers. A server record contains the following fields:

- **hostname** - String - hostname
- **managed\_host\_id** - Number - Id of the managed host the server host belongs to
- **private\_ip** - String - The private ip of this server
- **status** - String - The status of this server

## Response Sample

```
[
  {
    "hostname": "String",
    "managed_host_id": 42,
    "private_ip": "String",
    "server_id": 42,
    "status": "String"
  }
]
```

## GET /system/servers/{server\_id}

Retrieve a server host based on the supplied server ID.

Table 351. GET /system/servers/{server\_id} resource details

MIME Type
application/json

Table 352. GET /system/servers/{server\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 353. GET /system/servers/{server\_id} response codes

HTTP Response Code	Unique Code	Description
200		The requested server record has been retrieved.
404	1002	The requested server record with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.
500	1020	An error has occurred while trying to retrieve the requested server host with the given Id.

## Response Description

A server record containing the following fields:

- **email\_server\_address** - String - email server address
- **hostname** - String - hostname
- **managed\_host\_id** - Number - Id of the managed host the server host belongs to
- **private\_ip** - String - The private ip of this server
- **status** - String - The status of this server

## Response Sample

```
{
  "email_server_address": "String",
  "hostname": "String",
  "managed_host_id": 42,
  "private_ip": "String",
  "server_id": 42,
  "status": "String"
}
```

## POST /system/servers/{server\_id}

Updates an existing server.

Table 354. POST /system/servers/{server\_id} resource details

MIME Type
application/json

Table 355. POST /system/servers/{server\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server.



Table 356. POST /system/servers/{server\_id} request body details

Parameter	Data Type	MIME Type	Description	Sample
details	Object	application/json	Required - A server details record containing the following field:  <b>email_server_address</b> - String - email server address. Must be a valid server address that the server can connect to through port 25.	{ "email_server_address": "String" }

Table 357. POST /system/servers/{server\_id} response codes

HTTP Response Code	Unique Code	Description
200		The server record has been updated.
404	1002	The requested server record with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.
422	1006	Cannot connect to the mail server address on port 25.
500	1020	An error has occurred while trying to retrieve the requested server host with the given Id.

## Response Description

The updated server record containing the following fields:

- **email\_server\_address** - String - email server address.
- **hostname** - String - hostname
- **managed\_host\_id** - Number - Id of the managed host the server host belongs to
- **private\_ip** - String - The private ip of this server
- **status** - String - The status of this server

## Response Sample

```
{
  "email_server_address": "String",
  "hostname": "String",
  "managed_host_id": 42,
  "private_ip": "String",
  "server_id": 42,
  "status": "String"
}
```

## GET /system/servers/{server\_id}/firewall\_rules

Retrieve a list of access control firewall rules based on the supplied server ID.

Table 358. GET /system/servers/{server\_id}/firewall\_rules resource details

MIME Type
application/json

Table 359. GET /system/servers/{server\_id}/firewall\_rules request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 360. GET /system/servers/{server\_id}/firewall\_rules response codes

HTTP Response Code	Unique Code	Description
200		The rules records have been retrieved.
404	1002	The requested server with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.
500	1020	An error has occurred while trying to retrieve the requested access control firewall rules on the server with the given Id.

## Response Description

A list of the rules. Each rule record contains the following fields:

- **is\_any\_source\_ip** - Boolean - Whether any source IP is accepted
- **port\_range** - String - A port range in the format of start-end
- **port\_type** - String - one of: ANY, SINGLE, RANGE
- **protocol** - String - one of: ANY, TCP, UDP
- **single\_port** - String - A single port
- **source\_ip** - String - A specific IP address

## Response Sample

```
[
  {
    "is_any_source_ip": true,
    "port_range": "String",
    "port_type": "String <one of: ANY, SINGLE, RANGE>",
    "protocol": "String <one of: ANY, TCP, UDP>",
    "single_port": "String",
    "source_ip": "String"
  }
]
```

## PUT /system/servers/{server\_id}/firewall\_rules

Set the access control firewall rules based on the supplied server ID.

Table 361. PUT /system/servers/{server\_id}/firewall\_rules resource details

<b>MIME Type</b>
application/json

Table 362. PUT /system/servers/{server\_id}/firewall\_rules request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server.

Table 363. PUT /system/servers/{server\_id}/firewall\_rules request body details

Parameter	Data Type	MIME Type	Description	Sample
rules	Array<Object>	application/json	Required - A list of new rules in a JSON string. Each rule record contains the following field: <ul style="list-style-type: none"> <li><b>is_any_source_ip</b> - Boolean - Whether any source IP is accepted</li> <li><b>port_range</b> - String - A port range in the format of start-end</li> <li><b>port_type</b> - String - one of: ANY, SINGLE, RANGE</li> <li><b>protocol</b> - String - one of: ANY, TCP, UDP</li> <li><b>single_port</b> - String - A single port</li> <li><b>source_ip</b> - String - A specific IP address.</li> </ul>	[ { "is_any_source_ip": true, "port_range": "String", "port_type": "String <one of: ANY, SINGLE, RANGE>", "protocol": "String <one of: ANY, TCP, UDP>", "single_port": "String", "source_ip": "String" } ]

Table 364. PUT /system/servers/{server\_id}/firewall\_rules response codes

HTTP Response Code	Unique Code	Description
200		The rules have been updated.
404	1002	The requested server with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.

Table 364. PUT /system/servers/{server\_id}/firewall\_rules response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error has occurred while trying to set the access control firewall rules on the server with the given Id.

## Response Description

A list of the rules in a JSON string. Each rule contains the following fields:

- **is\_any\_source\_ip** - Boolean - Whether any source IP is accepted
- **port\_range** - String - A port range in the format of start-end
- **port\_type** - String - one of: ANY, SINGLE, RANGE
- **protocol** - String - one of: ANY, TCP, UDP
- **single\_port** - String - A single port
- **source\_ip** - String - A specific IP address

## Response Sample

```
[
  {
    "is_any_source_ip": true,
    "port_range": "String",
    "port_type": "String <one of: ANY, SINGLE, RANGE>",
    "protocol": "String <one of: ANY, TCP, UDP>",
    "single_port": "String",
    "source_ip": "String"
  }
]
```

## GET /system/servers/{server\_id}/network\_interfaces/ethernet

Retrieve a list of the ethernet network interfaces based on the supplied server ID.

Table 365. GET /system/servers/{server\_id}/network\_interfaces/ethernet resource details

MIME Type
application/json

Table 366. GET /system/servers/{server\_id}/network\_interfaces/ethernet request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 366. GET /system/servers/{server\_id}/network\_interfaces/ethernet request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 367. GET /system/servers/{server\_id}/network\_interfaces/ethernet response codes

HTTP Response Code	Unique Code	Description
200		A list of the ethernet network interfaces have been retrieved.
404	1002	The requested server with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.
500	1020	An error has occurred while trying to retrieve the ethernet interfaces on the server with the given Id.

## Response Description

A list of the ethernet network interfaces. Each ethernet network interface contains the following fields:

- **device\_name** - String - The name of the network interface
- **desc** - String - The description of the network interface
- **role** - String - The role of the network interface. one of: regular, management, hacrossover, hacrossover\_disabled, monitor, disabled
- **ipversion** - String - The version of the ip address configured on the network interface. one of: ipv4, ipv6
- **ip** - String - The ip configured on the network interface
- **mask** - String - The netmask configured on the network interface
- **gateway** - String - The gateway configured on the network interface
- **is\_auto\_ip** - Boolean - Is the ip auto configured
- **is\_cable\_linked** - Boolean - Is the network interface cable linked.
- **is\_moving\_config\_with\_active\_ha** - Boolean - Will apply the same settings to a new active HA server during failover.

- **hacrossover\_params** - String - A map of key-value pairs of HA crossover parameters if the network interface is used for HA crossover.

## Response Sample

```
[
  {
    "desc": "String",
    "device_name": "String",
    "gateway": "String",
    "hacrossover_params": {
      "String": "String"
    },
    "ip": "String",
    "ipversion": "String <one of: ipv4, ipv6>",
    "is_auto_ip": true,
    "is_cable_linked": true,
    "is_moving_config_with_active_ha": true,
    "mask": "String",
    "role": "String <one of: regular,
      management,
      hacrossover,
      hacrossover_disabled,
      monitor,
      disabled,
      slave,
      slave_disabled>",
  }
]
```

## POST /system/servers/{server\_id}/network\_interfaces/ethernet/{device\_name}

Update an ethernet network interface based on the supplied server ID and device name.

Table 368. POST /system/servers/{server\_id}/network\_interfaces/ethernet/{device\_name} resource details

MIME Type
application/json

Table 369. POST /system/servers/{server\_id}/network\_interfaces/ethernet/{device\_name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server.
device_name	path	Required	String	text/plain	Required - The name of an existing ethernet network interface. The interface cannot be the management interface, HA crossover interface or a slave of a bonded interface.

Table 370. POST /system/servers/{server\_id}/network\_interfaces/ethernet/{device\_name} request body details

Parameter	Data Type	MIME Type	Description	Sample
details	Object	application/json	<p>Required - An ethernet network interface record containing the following fields:</p> <p><b>role</b> - String - The role of the network interface. Must be one of: regular, monitor, disabled</p> <p><b>ipversion</b> - String - The version of the ip address configured on the network interface. one of: ipv4, ipv6</p> <p><b>ip</b> - String - The ip configured on the network interface. Required when ipversion is ipv4 or (ipversion is ipv6 and is_auto_ip is false). The subnet computed from the ip and the mask must not be the same subnet configured on the management interface.</p> <p><b>mask</b> - String - The netmask configured on the network interface. Required when ipversion is ipv4. The subnet computed from the ip and the mask must not be the same subnet configured on the management interface.</p> <p><b>gateway</b> - String - The gateway configured on the network interface. Optional when ipversion is ipv4. Empty value means the network interface will use the default gateway. Does not need in ipv6</p> <p><b>is_auto_ip</b> - Boolean - Is the ip auto configured. Required</p> <p><b>is_moving_config_with_active_ha</b> - Boolean - Will apply the same settings to a new active HA server during failover. Can be true only when the server host is an active HA server host</p>	<pre>{ "gateway": "String", "ip": "String", "ipversion": "String &lt;one of: ipv4, ipv6&gt;", "is_moving_config_with_active_ha": true, "mask": "String", "role": "String &lt;one of: regular, management, hacrossover, hacrossover_disabled, monitor, disabled, slave, slave_disabled&gt;" }</pre>

Table 371. POST /system/servers/{server\_id}/network\_interfaces/ethernet/{device\_name} response codes

HTTP Response Code	Unique Code	Description
200		The network interface has been updated.
404	1002	The requested server with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.
500	1020	An error has occurred while trying to update the specified ethernet interfaces on the server with the given Id.

## Response Description

The updated ethernet network interface containing the following fields:

- **device\_name** - String - The name of the network interface
- **role** - String - The role of the network interface. one of: regular, management, hacrossover, hacrossover\_disabled, monitor, disabled
- **ipversion** - String - The version of the ip address configured on the network interface. one of: ipv4, ipv6

- **ip** - String - The ip configured on the network interface
- **mask** - String - The netmask configured on the network interface
- **gateway** - String - The gateway configured on the network interface
- **is\_auto\_ip** - Boolean - Is the ip auto configured
- **is\_moving\_config\_with\_active\_ha** - Boolean - Will apply the same settings to a new active HA server during failover.

## Response Sample

```
{
  "desc": "String",
  "device_name": "String",
  "gateway": "String",
  "hacrossover_params": {
    "String": "String"
  },
  "ip": "String",
  "ipversion": "String <one of: ipv4, ipv6>",
  "is_auto_ip": true,
  "is_cable_linked": true,
  "is_moving_config_with_active_ha": true,
  "mask": "String",
  "role": "String <one of: regular,
management,
hacrossover,
hacrossover_disabled,
monitor,
disabled,
slave,
slave_disabled>",
}
```

## GET /system/servers/{server\_id}/network\_interfaces/bonded

Retrieve a list of the bonded network interfaces based on the supplied server ID.

Table 372. GET /system/servers/{server\_id}/network\_interfaces/bonded resource details

MIME Type
application/json

Table 373. GET /system/servers/{server\_id}/network\_interfaces/bonded request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.



Table 373. GET /system/servers/{server\_id}/network\_interfaces/bonded request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 374. GET /system/servers/{server\_id}/network\_interfaces/bonded response codes

HTTP Response Code	Unique Code	Description
200		A list of the bonded network interfaces have been retrieved.
404	1002	The requested server with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.
500	1020	An error has occurred while trying to retrieve the bonded interfaces on the server with the given Id.

## Response Description

A list of the bonded network interfaces. Each record contains the following fields:

- **device\_name** - String - The name of the network interface
- **desc** - String - The description of the network interface
- **role** - String - The role of the network interface. one of: regular, management, hacrossover, hacrossover\_disabled, monitor, disabled
- **ipversion** - String - The version of the ip address configured on the network interface. one of: ipv4, ipv6
- **ip** - String - The ip configured on the network interface
- **mask** - String - The netmask configured on the network interface
- **gateway** - String - The gateway configured on the network interface
- **is\_auto\_ip** - Boolean - Is the ip auto configured
- **is\_cable\_linked** - Boolean - Is the network interface cable linked.
- **is\_moving\_config\_with\_active\_ha** - Boolean - Will apply the same settings to a new active HA server during failover.

- **hacrossover\_params** - String - A map of key-value pairs of HA crossover parameters if the network interface is used for HA crossover.
- **bonding\_opts** - String - The bonding options configured on the bonded network interface
- **slaves** - List - The slaves of the bonded network interface. Each slave record contains the follow fields:
  - **device\_name** - String - The name of the slave interface
  - **desc** - String - The description of the slave interface
  - **role** - String - The role of the slave interface. one of: slave, slave\_disabled
  - **is\_cable\_linked** - Boolean - Is the slave interface cable linked.

## Response Sample

```
[
  {
    "bonding_opts": "String",
    "desc": "String",
    "device_name": "String",
    "gateway": "String",
    "hacrossover_params": {
      "String": "String"
    },
    "ip": "String",
    "ipversion": "String <one of: ipv4, ipv6>",
    "is_auto_ip": true,
    "is_cable_linked": true,
    "is_moving_config_with_active_ha": true,
    "mask": "String",
    "role": "String <one of: regular,
              management,
              hacrossover,
              hacrossover_disabled,
              monitor,
              disabled,
              slave,
              slave_disabled>",
    "slaves": [
      {
        "desc": "String",
        "device_name": "String",
        "is_cable_linked": true,
        "role": "String <one of: regular,
                  management,
                  hacrossover,
                  hacrossover_disabled,
                  monitor,
                  disabled,
                  slave,
                  slave_disabled>"
      }
    ]
  }
]
```

## POST /system/servers/{server\_id}/network\_interfaces/bonded/{device\_name}

Update an existing bonded network interface.

Table 375. POST /system/servers/{server\_id}/network\_interfaces/bonded/{device\_name} resource details

MIME Type
application/json

Table 376. POST /system/servers/{server\_id}/network\_interfaces/bonded/{device\_name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
server_id	path	Required	Number (Integer)	text/plain	Required - The id of the server.
device_name	path	Required	String	text/plain	Required - The name of an existing bonded network interface. The interface cannot be the management interface or HA crossover interface

Table 377. POST /system/servers/{server\_id}/network\_interfaces/bonded/{device\_name} request body details

Parameter	Data Type	MIME Type	Description	Sample
details	Object	application/json	<p>Required - The details of the bonded network interface containing the following fields:</p> <p><b>role</b> - String - The role of the network interface. Must be one of: regular, monitor, disabled</p> <p><b>ipversion</b> - String - The version of the ip address configured on the network interface. one of: ipv4, ipv6</p> <p><b>ip</b> - String - The ip configured on the network interface. Required when ipversion is ipv4 or (ipversion is ipv6 and is_auto_ip is false). The subnet computed from the ip and the mask must not be the same subnet configured on the management interface.</p> <p><b>mask</b> - String - The netmask configured on the network interface. Required when ipversion is ipv4. The subnet computed from the ip and the mask must not be the same subnet configured on the management interface.</p> <p><b>gateway</b> - String - The gateway configured on the network interface. Optional when ipversion is ipv4. Empty value means the network interface will use the default gateway. Does not need in ipv6</p> <p><b>is_auto_ip</b> - Boolean - Is the ip auto configured. Required</p> <p><b>is_moving_config_with_active_ha</b> - Boolean - Will apply the same settings to a new active HA server during failover. Can be true only when the server host is an active HA server host</p> <p><b>bonding_opts</b> - String - The bonding options configured on the bonded network interface</p>	<pre>{ "bonding_opts": "String", "gateway": "String", "ip": "String", "ipversion": "String &lt;one of: ipv4, ipv6&gt;", "is_moving_config_with_active_ha": true, "mask": "String", "role": "String &lt;one of: regular, management, haccrossover, haccrossover_disabled, monitor, disabled, slave, slave_disabled&gt;", "slaves": [ { "device_name": "String", "role": "String &lt;one of: regular, management, haccrossover, haccrossover_disabled, monitor, disabled, slave, slave_disabled&gt;" } ] }</pre>

Table 378. POST /system/servers/{server\_id}/network\_interfaces/bonded/{device\_name} response codes

HTTP Response Code	Unique Code	Description
200		The network interface has been updated.
404	1002	The requested server with the given server_id cannot be found.
422	1005	One or more parameters are invalid in request.
500	1020	An error has occurred while trying to update the specified bonded interfaces on the server with the given Id.

## Response Description

The updated bonded network interface containing the following fields:

- **device\_name** - String - The name of the network interface
- **role** - String - The role of the network interface. one of: regular, management, haccrossover, haccrossover\_disabled, monitor, disabled

- **ipversion** - String - The version of the ip address configured on the network interface. one of: ipv4, ipv6
- **ip** - String - The ip configured on the network interface
- **mask** - String - The netmask configured on the network interface
- **gateway** - String - The gateway configured on the network interface
- **is\_auto\_ip** - Boolean - Is the ip auto configured
- **is\_moving\_config\_with\_active\_ha** - Boolean - Will apply the same settings to a new active HA server during failover.
- **bonding\_opts** - String - The bonding options configured on the bonded network interface

## Response Sample

```
{
  "bonding_opts": "String",
  "desc": "String",
  "device_name": "String",
  "gateway": "String",
  "hacrossover_params": {
    "String": "String"
  },
  "ip": "String",
  "ipversion": "String <one of: ipv4, ipv6>",
  "is_auto_ip": true,
  "is_cable_linked": true,
  "is_moving_config_with_active_ha": true,
  "mask": "String",
  "role": "String <one of: regular,
    management,
    hacrossover,
    hacrossover_disabled,
    monitor,
    disabled,
    slave,
    slave_disabled>",
  "slaves": [
    {
      "desc": "String",
      "device_name": "String",
      "is_cable_linked": true,
      "role": "String <one of: regular,
        management,
        hacrossover,
        hacrossover_disabled,
        monitor,
        disabled,
        slave,
        slave_disabled>"
    }
  ]
}
```



---

## Chapter 6. Previous REST API versions

Use this reference if you are using REST API version 2.0 or previous.

---

### REST API V4.0 References

Each API reference provides information about the parameters, mime type, stability, and responses for each endpoint.

#### Ariel endpoints

Use the references for REST API V4 Ariel endpoints.

##### GET /ariel/databases

Retrieve Ariel database names

Table 379. GET /ariel/databases resource details

<b>MIME Type</b>
application/json

Table 380. GET /ariel/databases request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 381. GET /ariel/databases response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of Ariel databases.

#### Response Description

The names of the available Ariel databases.

## Response Sample

```
[  
  "String"  
]
```

## GET /ariel/databases/{database\_name}

Retrieve the columns defined for a specific Ariel database.

This is the set of columns that can be explicitly named in the column list of a SELECT query.

Table 382. GET /ariel/databases/{database\_name} resource details

MIME Type
application/json

Table 383. GET /ariel/databases/{database\_name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
database_name	path	Required	String	text/plain	Required. The name of the Ariel database that contains the columns that you want to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 384. GET /ariel/databases/{database\_name} response codes

HTTP Response Code	Unique Code	Description
200		The database columns were retrieved.
404	1002	The database does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the database columns.



## Response Description

A list of columns that are defined for the specified database. Multiple properties of each column are returned. For example, the column name or an indication that the column is indexable.

## Response Sample

```
{
  "columns": [
    {
      "argument_type": "String",
      "indexable": true,
      "name": "String"
    }
  ]
}
```

## GET /ariel/searches

Retrieve Ariel search\_ids.

Retrieve the list of Ariel searches. This includes search\_ids for completed and active searches.

Table 385. GET /ariel/searches resource details

MIME Type
application/json

Table 386. GET /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 387. GET /ariel/searches response codes

HTTP Response Code	Unique Code	Description
200		The search list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of searches.

## Response Description

A list of search IDs.

## Response Sample

```
[  
  "String"  
]
```

## POST /ariel/searches

Create a new asynchronous Ariel search

Creates a new Ariel search as specified by the Ariel Query Language (AQL) query expression. Searches are executed asynchronously. A reference to the search\_id is returned and should be used in subsequent API calls to determine the status of the search and retrieve the results once it is complete.

This endpoint only accepts SELECT and RUN query expressions.

Queries are applied to the range of data in a certain time interval. By default this time interval is the last 60 seconds. An alternative time interval can be specified by specifying them as part of the query expression. For further information, see the AQL reference.

Table 388. POST /ariel/searches resource details

MIME Type
application/json

Table 389. POST /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
query_expression	query	Required	String	text/plain	Required - The AQL query to execute.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 390. POST /ariel/searches response codes

HTTP Response Code	Unique Code	Description
201		A new Ariel search was successfully created.
409	1004	The search could not be created, the requested search ID provided in the query_expression is already in use. Please use a unique search ID (or allow one to be generated).
422	2000	The query_expression contains invalid AQL syntax.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create a new search.

## Response Description

Information about the specified search, including the `search_id`. Use the `search_id` to access or manipulate the search with the other API endpoints.

If the exact search being created was already recently created, the response message will return a reference to the original `search_id` rather than creating a new search.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## GET /ariel/searches/{search\_id}

Retrieve information about an Ariel search

Retrieve status information for a search, based on the `search_id` parameter. The same informational fields are returned regardless of whether the search is in progress or is complete.

Table 391. GET /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 392. GET /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The identifier for an Ariel search.

Table 392. GET /ariel/searches/{search\_id} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 393. GET /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search information was retrieved.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search information.

## Response Description

Information about the specified search, including the search status.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## POST /ariel/searches/{search\_id}

Update an Ariel search.

Update details for an Ariel search. You can update searches in the following ways:

- To cancel an active search, set the **status** parameter to CANCELED. This stops the search and keeps any search results that were collected before the search was canceled.
- The results for a completed search can be saved by setting the **save\_results** parameter to true. This ensures that the search is not automatically removed when it expires in accordance with the retention policy.

The Ariel server uses an internal retention policy to manage available disk space. Searches might be deleted automatically, according to the settings of the retention policy. Searches with saved results are not automatically reclaimed by the server and are therefore retained. A search can be explicitly deleted by using the DELETE /searches/{search\_id} endpoint.

Note: Saving too many search results might result in insufficient disk space to process new searches.

Table 394. POST /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 395. POST /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The ID of the search to update.
save_results	query	Optional	String	text/plain	Optional. The only accepted value is true. If this value is provided, the search results will not be deleted by the search expiration removal process.
status	query	Optional	String	text/plain	Optional. The only accepted value is CANCELED. If this value is provided, the search will be canceled.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 396. POST /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search was updated.
404	1002	The search does not exist.
409	1008	The current status of the search prevented the search results from being saved.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to update the search.

## Response Description

Information about the specified search that was updated.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## DELETE /ariel/searches/{search\_id}

Delete an Ariel search

Deletes an Ariel search. This discards any results that were collected and stops the search if it is currently processing. This search is deleted regardless of whether the results were saved.

Table 397. DELETE /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 398. DELETE /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required - The search_id of the search to delete.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 399. DELETE /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
202		The delete request has been accepted.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to delete the search.

## Response Description

Information about the deleted search

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
}
```

```

    "save_results": true,
    "search_id": "String",
    "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}

```

## GET /ariel/searches/{search\_id}/results

Retrieves search results in the requested format.

Retrieve the results of the Ariel search that is identified by the **search\_id**. The Accepts request header indicates the format of the result. The format can be JSON, CSV, XML, or tabular text.

By default, all query result records are returned. To restrict the results to a contiguous subset of the records, you can supply a Range header to specify the inclusive range of records to be returned.

This end-point works with query results that are generated by AQL query expressions. This endpoint might not work as expected for results that are generated by other means. Search results might not be retrievable for searches that are created on the Console.

The response samples are for the following query: Select sourceIP, destinationIP from events.

Table 400. GET /ariel/searches/{search\_id}/results resource details

MIME Type
application/json application/csv text/table application/xml

Table 401. GET /ariel/searches/{search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	The ID of the search criteria for the returned results.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 402. GET /ariel/searches/{search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The search results were retrieved.
404	1002	The search does not exist.
404	1003	Search results not found. The search is still in progress.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search results.



## Response Description

The search results for the specified search\_id. The format that is used to encapsulate the data depends on the format specified in the Accept header for this request.

## Response Sample

```
{
  "events": [
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    },
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    }
  ]
}
```

## Asset model endpoints

Use the references for REST API V4 Asset Model endpoints.

### GET /asset\_model/assets

List all assets found in the model.

Table 403. GET /asset\_model/assets resource details

MIME Type
application/json

Table 404. GET /asset\_model/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 405. GET /asset\_model/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
500	1020	The server encountered an error while trying to retrieve the assets.

## Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[{"id": 42,
  "domain_id": 42,
  "interfaces": [{"first_seen_scanner": 42,
    "id": 42,
    "first_seen_profiler": 42,
    "created": 42,
    "last_seen_profiler": 42,
    "last_seen_scanner": 42,
    "mac_address": "String",
    "ip_addresses": [{"first_seen_scanner": 42,
      "id": 42,
      "first_seen_profiler": 42,
      "created": 42, "network_id": 42,
      "value": "String",
      "last_seen_profiler": 42,
      "last_seen_scanner": 42,
      "type": "String"}]}],
  "properties": [{"id": 42,
    "name": "String",
    "value": "String",
    "last_reported": 42,
    "type_id": 42,
    "last_reported_by": "String"}]}]
```

## POST /asset\_model/assets/{asset\_id}

Update an asset with several pertinent pieces of information.

Update an asset with several pertinent pieces of information. The **asset\_id** tag is mandatory, and is the unique identifier for an asset. This field is available through the **/asset\_model/assets** or **/asset\_model/saved\_searches/{saved\_search\_id}/results** query. To update properties, the property type id which is available through the **/asset\_model/properties** query should be provided along with the new value. See the sample provided demonstrating an example asset update.

Table 406. POST /asset\_model/assets/{asset\_id} resource details

MIME Type
text/plain

Table 407. *POST /asset\_model/assets/{asset\_id}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
asset_id	path	Required	String	text/plain	Unique identifier of the asset to update.

Table 408. *POST /asset\_model/assets/{asset\_id}* request body details

Parameter	Data Type	MIME Type	Description	Sample
asset	JSON	application/json	JSON representation of an asset.	{ "properties": [ { "type_id": 1001, "value": "given name value" }, { "type_id": 1002, "value": "unified name value" } ] }

Table 409. *POST /asset\_model/assets/{asset\_id}* response codes

HTTP Response Code	Unique Code	Description
202		The request to update the asset was successful. The update will take place when the asset profile application receives the request.
422	1005	One or more of the requested property updates were invalid.
500	1020	The server encountered an error registering the update with the asset profile application.

## Response Description

Information about the asset that was updated.

## Response Sample

String

## GET /asset\_model/properties

Get a list of available asset property types that can be used.

Get a list of available asset property types that can be used or applied against the */asset\_model/assets* endpoint.

Table 410. *GET /asset\_model/properties* resource details

<b>MIME Type</b>
application/json

Table 411. GET /asset\_model/properties request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 412. GET /asset\_model/properties response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of asset property types completed successfully.
500	1020	An error occurred while trying to retrieve the list of asset property types.

## Response Description

List of asset properties. Per asset property type: id and name that make up this asset property type.

## Response Sample

```
[
  {
    "custom": true,
    "data_type": "String",
    "display": true,
    "id": 42,
    "name": "String",
    "state": 42
  }
]
```

## GET /asset\_model/saved\_searches

Get a list of saved searches that can be used.

Get a list of saved searches that can be used or applied against the `/asset_model/saved_searches/{saved_search_id}/results` query.

Table 413. GET /asset\_model/saved\_searches resource details

<b>MIME Type</b>
application/json

Table 414. GET /asset\_model/saved\_searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 415. GET /asset\_model/saved\_searches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully.
500	1020	The server encountered an error while trying to retrieve the list of saved searches.

## Response Description

List of saved searches. Per saved search: id, name and list of filters that make up this saved search

## Response Sample

```
[
  {
    "columns": [
      {
        "name": "String",
```

```

        "type": "String"
    },
    ],
    "description": "String",
    "filters": [
        {
            "operator": "String",
            "parameter": "String",
            "value": "String"
        }
    ],
    "id": 42,
    "name": "String"
}
]

```

## GET /asset\_model/saved\_searches/{saved\_search\_id}/results

Retrieves a list of assets based on the results of an asset saved search.

Table 416. GET /asset\_model/saved\_searches/{saved\_search\_id}/results resource details

MIME Type
application/json

Table 417. GET /asset\_model/saved\_searches/{saved\_search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
saved_search_id	path	Required	String	text/plain	Unique identifier of the saved search used to retrieve assets.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 418. GET /asset\_model/saved\_searches/{saved\_search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
422	1005	The unique identifier of the saved search provided was invalid.

Table 418. GET /asset\_model/saved\_searches/{saved\_search\_id}/results response codes (continued)

HTTP Response Code	Unique Code	Description
500	1003	The server encountered an error executing the saved search.

## Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[
  {
    "domain_id": 42,
    "id": 42,
    "interfaces": [
      {
        "created": 42,
        "first_seen_profiler": 42,
        "first_seen_scanner": 42,
        "id": 42,
        "ip_addresses": [
          {
            "created": 42,
            "first_seen_profiler": 42,
            "first_seen_scanner": 42,
            "id": 42,
            "last_seen_profiler": 42,
            "last_seen_scanner": 42,
            "network_id": 42,
            "type": "String",
            "value": "String"
          }
        ],
        "last_seen_profiler": 42,
        "last_seen_scanner": 42,
        "mac_address": "String"
      }
    ],
    "properties": [
      {
        "id": 42,
        "last_reported": 42,
        "last_reported_by": "String",
        "name": "String",
        "type_id": 42,
        "value": "String"
      }
    ]
  }
]
```

## Authentication endpoints

Use the references for REST API V4 authentication endpoints.

## POST /auth/logout

Invoke this method as an authorized user and your session is invalidated.

Table 419. POST /auth/logout resource details

<b>MIME Type</b>
text/plain

There are no parameters for this endpoint.

Table 420. POST /auth/logout response codes

HTTP Response Code	Unique Code	Description
200		The session was invalidated.

## Response Description

Returns true. Throws exception upon failure.

## Response Sample

true

## Help endpoints

Use the references for REST API V4 Help endpoints.

## GET /help/capabilities

List all QRadar API capabilities

The response will contain all available RESTful resources We allow every authenticated user to access this method, but restrict the output based on their user capabilities

Table 421. GET /help/capabilities resource details

<b>MIME Type</b>
application/json

Table 422. GET /help/capabilities request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
categories	query	Optional	Array<String>	application/json	Optional - Restrict your search to this list of capabilities
paths	query	Optional	Array<String>	application/json	Optional - Restrict your search to these paths only
httpMethods	query	Optional	Array<String>	application/json	Optional - Restrict your search to these HTTP methods
version	query	Optional	String	text/plain	Optional - Restrict your search to this version (or below)
showExperimental	query	Optional	Boolean	text/plain	Optional - If true, we include experimental endpoints (default is true)
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.



Table 422. GET /help/capabilities request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 423. GET /help/capabilities response codes

HTTP Response Code	Unique Code	Description
200		The API capabilities list was retrieved.
422	1001	Invalid input
422	1002	Our internal mapping has an unexpected structure or contains an invalid element value
500	1003	A generic error has occurred while retrieving our capabilities

## Response Description

Endpoints you are able to access, mapped against versions they belong to. If full content is not requested, values will be null.

## Response Sample

```
{
  "categories": [
    {
      "apis": [
        {
          "httpMethod": "String <one of: OPTIONS,
            GET,
            HEAD,
            POST,
            PUT,
            DELETE,
            TRACE,
            CONNECT,
            PATCH>",
          "operations": [
            {
              "additionalFiltering": true,
              "deprecated": true,
              "description": "String",
              "errorResponses": [
                {
                  "code": 42,
                  "description": "String",
                  "uniqueCode": 42
                }
              ]
            },
            {
              "httpMethod": "String",
              "lastSupportedVersion": "String",
              "parameters": [
                {
                  "allowMultiple": true,
                  "defaultValue": "String",
                  "description": "String",

```

```

        "name": "String",
        "pathIndex": 42,
        "required": true,
        "source": "String",
        "supportedContentTypes": [
            {
                "dataType": "String",
                "mimeType": "String",
                "sample": "String"
            }
        ]
    },
    "removalTarget": "String",
    "removed": true,
    "responseClass": "String",
    "responseDescription": {
        "description": "String",
        "properties": [
            {
                "description": "String",
                "name": "String"
            }
        ]
    },
    "successResponses": [
        {
            "code": 42,
            "description": "String"
        }
    ],
    "summary": "String",
    "supportedContentTypes": [
        {
            "dataType": "String",
            "mimeType": "String",
            "sample": "String"
        }
    ],
    "version": "String",
    "visibility": "String"
    },
    "path": "String"
    },
    "path": "String"
    },
    "path": "String"
}

```

## QRadar Vulnerability Manager endpoints

Use the references for REST API V4 QRadar Vulnerability Manager endpoints.

### GET /qvm/assets

List the assets with discovered vulnerabilities present in the asset model. The response contains all available RESTful resources

Table 424. GET /qvm/assets resource details

MIME Type
application/json

Table 425. GET /qvm/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 426. GET /qvm/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by asset completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of assets data

## Response Sample

### GET /qvm/filters

Get a list of the allowable filters that can be used or applied against /qvm endpoints.

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 427. GET /qvm/filters resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 428. GET /qvm/filters response codes

HTTP Response Code	Unique Code	Description
200		The search executed successfully
420	9102	An error occurred while executing the search

## Response Description

list of Filters.

## Response Sample

### GET /qvm/network

List the networks present in the asset model with vulnerabilities present. The response contains all available RESTful resources

Table 429. GET /qvm/network resource details

<b>MIME Type</b>
application/json

Table 430. GET /qvm/network request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 431. GET /qvm/network response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by network completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of network related data

## Response Sample

### GET /qvm/openservices

List the open services present in the asset model with vulnerabilities present. The response contains all available RESTful resources

Table 432. GET /qvm/openservices resource details

<b>MIME Type</b>
application/json

Table 433. GET /qvm/openservices request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name

Table 433. GET /qvm/openservices request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 434. GET /qvm/openservices response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by open service completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of open services related data

## Response Sample

### GET /qvm/savedsearches

Get a list of saved searches that can be applied against /qvm endpoints.

A list of saved searches that can be applied against the following endpoints:

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 435. GET /qvm/savedsearches resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 436. GET /qvm/savedsearches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully
420	9103	An error occurred while trying to retrieve the list of saved searches

## Response Description

list of saved searches. Per saved search: id, name and list fo filters that make up this saved search

## Response Sample

### POST /qvm/tickets/assign

Update the remediation ticket for the assigned vulnerability

Table 437. POST /qvm/tickets/assign resource details

<b>MIME Type</b>
application/json

Table 438. POST /qvm/tickets/assign request body details

Parameter	Data Type	MIME Type	Description	Sample
ticket	JSON	application/json	<p>'ticketId': required.</p> <p>'priority' one of required : Critical, Major, Minor, Warning, Informational.</p> <p>'status' one of required : Opened, Fixed, Re-Opened, Closed .</p> <p>'dueDate' Optional : yyyy-MM-dd HH:mm:ss.</p> <p>'assignedUser' required : valid QRadar user account name or a valid email.</p> <p>'comment' Optional : text.</p> <p>'commentUser' Optional : valid QRadar user account name, if not included will default current API user.</p>	[ { "ticketId":"1000", "status":"Opened", "priority":"Critical", "dueDate":"2015-01-04 12:00:00", "assignedUser":"admin", "comment":"testComment", "commentUser":"admin" } ]

Table 439. POST /qvm/tickets/assign response codes

HTTP Response Code	Unique Code	Description
200		The request to assign a ticket completed successfully
420	9104	An error occurred while trying to assign a ticket due to invalid arguments

## Response Description

success message if update succeed

## Response Sample

### GET /qvm/vulninstances

List the Vulnerability Instances present in the asset model. The response will contain all available RESTful resources

Table 440. GET /qvm/vulninstances resource details

<b>MIME Type</b>
application/json

Table 441. GET /qvm/vulninstances request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 442. GET /qvm/vulninstances response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by instance completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability instance data

## Response Sample

### GET /qvm/vulns

List the Vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 443. GET /qvm/vulns resource details

<b>MIME Type</b>
application/json

Table 444. GET /qvm/vulns request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name

Table 444. GET /qvm/vulns request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 445. GET /qvm/vulns response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability data

## Response Sample

## Reference data endpoints

Use the references for REST API V4 reference data endpoints.

### GET /reference\_data/map\_of\_sets

Retrieve a list of all reference map of sets.

Table 446. GET /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 447. GET /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.



Table 447. GET /reference\_data/map\_of\_sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 448. GET /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

## Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## DELETE /reference\_data/map\_of\_sets/{name}

Remove a map of sets or purge its contents.

Table 449. DELETE /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 450. DELETE /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 451. DELETE /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map of sets does not exist
409	1004	The reference map of sets could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

## Response Description

If the reference map of sets was removed nothing is returned, otherwise information about the reference map of sets that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/map\_of\_sets/{name}

Return the reference map of sets identified by name.

Return the reference map of sets identified by **name**. If provided, **limit** specifies the number of records to return that starts at the record specified by **offset**. If not specified, then the first 20 records are returned.

Table 452. GET /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 453. GET /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 454. GET /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid

Table 454. GET /reference\_data/map\_of\_sets/{name} response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to retrieve the reference map of sets

## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": [
      {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    ]
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name}/{key}

Remove a value from a reference map of sets.

Table 455. DELETE /reference\_data/map\_of\_sets/{name}/{key} resource details

MIME Type
application/json

Table 456. DELETE /reference\_data/map\_of\_sets/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove

Table 456. DELETE /reference\_data/map\_of\_sets/{name}/{key} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 457. DELETE /reference\_data/map\_of\_sets/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

## Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/map\_of\_sets/{name}

Add or update an element in a reference map of sets.

Table 458. POST /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 459. POST /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 460. POST /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map of sets

### Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/map\_of\_sets

Create a new reference map of sets.

Table 461. POST /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 462. POST /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 462. POST /reference\_data/map\_of\_sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 463. POST /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps

Retrieve a list of all reference maps.

Table 464. GET /reference\_data/maps resource details

MIME Type
application/json



Table 465. GET /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 466. GET /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

## Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## DELETE /reference\_data/maps/{name}

Remove a reference map or purge its contents.

Table 467. DELETE /reference\_data/maps/{name} resource details

<b>MIME Type</b>
application/json

Table 468. DELETE /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 469. DELETE /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map does not exist
409	1004	The reference map could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

## Response Description

If the reference map was removed nothing is returned, otherwise information about the reference map that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps/{name}

Retrieve the reference map identified by name.

Retrieve the reference map identified by **name**. If provided, **limit** specifies the number of records to return that start at the record specified by **offset**. If not specified, then the first 20 records are returned.

Table 470. GET /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 471. GET /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 471. GET /reference\_data/maps/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 472. GET /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/maps/{name}/{key}

Remove a value from a reference map.

Table 473. DELETE /reference\_data/maps/{name}/{key} resource details

MIME Type
application/json

Table 474. DELETE /reference\_data/maps/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 475. DELETE /reference\_data/maps/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

## Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/maps/{name}

Add or update an element in a reference map.

Table 476. POST /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 477. POST /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 478. POST /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/maps

Create a new reference map.

Table 479. POST /reference\_data/maps resource details

MIME Type
application/json

Table 480. POST /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.

Table 480. POST /reference\_data/maps request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 481. POST /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/sets/bulk\_load/{name}

Add or update data in a reference set.

Table 482. POST /reference\_data/sets/bulk\_load/{name} resource details

MIME Type
application/json



Table 483. POST /reference\_data/sets/bulk\_load/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 484. POST /reference\_data/sets/bulk\_load/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Array	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 485. POST /reference\_data/sets/bulk\_load/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

## Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/sets

Retrieve a list of all reference sets.

Table 486. GET /reference\_data/sets resource details

<b>MIME Type</b>
application/json

Table 487. GET /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 488. GET /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

## Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "number_of_elements": 42,
```

```

        "time_to_live": "String",
        "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
    }
]

```

## DELETE /reference\_data/sets/{name}

Remove a reference set or purge its contents.

Table 489. DELETE /reference\_data/sets/{name} resource details

<b>MIME Type</b>
application/json

Table 490. DELETE /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 491. DELETE /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had its contents purged
204		The reference set has been removed
404	1002	The reference set does not exist
409	1004	The reference set could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference set

## Response Description

If the reference set was removed nothing is returned, otherwise information about the reference set that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/sets/{name}

Retrieve the reference set identified by name.

Retrieve the reference set identified by **name**. If provided, **limit** specifies the number of records to return that start at the record specified by **offset**. If not specified, then the first 20 records are returned.

Table 492. GET /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 493. GET /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 493. GET /reference\_data/sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 494. GET /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": [
    {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  ],
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/{name}

Add or update an element in a reference set.

Table 495. POST /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 496. *POST /reference\_data/sets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 497. *POST /reference\_data/sets/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update an element in the reference set

## Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
```

```

    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## DELETE /reference\_data/sets/{name}/{value}

Remove a value from a reference set.

Table 498. DELETE /reference\_data/sets/{name}/{value} resource details

<b>MIME Type</b>
application/json

Table 499. DELETE /reference\_data/sets/{name}/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 500. DELETE /reference\_data/sets/{name}/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had an value removed. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets

Create a new reference set.

Table 501. POST /reference\_data/sets resource details

MIME Type
application/json

Table 502. POST /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"



Table 502. POST /reference\_data/sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 503. POST /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables

Retrieve a list of all reference tables.

Table 504. GET /reference\_data/tables resource details

MIME Type
application/json

Table 505. GET /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 506. GET /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "key_name_types": {
      "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    },
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## DELETE /reference\_data/tables/{name}

Remove a reference table or purge its contents.

Table 507. DELETE /reference\_data/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 508. DELETE /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 509. DELETE /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had its contents purged
204		The reference table has been removed
404	1002	The reference table does not exist
409	1004	The reference table could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

## Response Description

If the table was removed nothing is returned, otherwise information about the reference table that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables/{name}

Return the reference table identified by name.

Return the reference table identified by **name**. If provided, **limit** specifies the number of records to return that start at the record specified by **offset**. If not specified, then the first 20 records are returned.

Table 510. GET /reference\_data/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 511. GET /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 512. GET /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "String": {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key}

Remove a value from a reference table.

Table 513. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} resource details

MIME Type
application/json

Table 514. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from

Table 514. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
outer_key	path	Required	String	text/plain	Required - The outer key of the value to remove
inner_key	path	Required	String	text/plain	Required - The inner key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 515. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference table value

## Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
```

```

    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## POST /reference\_data/tables/{name}

Add or update an element in a reference table.

The value to be added must be of the appropriate type: either the type that corresponds to the innerKey predefined for the reference table, or the default elementType of the reference table

Table 516. POST /reference\_data/tables/{name} resource details

MIME Type
application/json

Table 517. POST /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to add or update an element in
outer_key	query	Required	String	text/plain	Required - The outer key for the element to add or update
inner_key	query	Required	String	text/plain	Required - The inner key for the element to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 518. *POST /reference\_data/tables/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table

## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/tables

Create a new reference table.

Create a new reference table.

Table 519. *POST /reference\_data/tables* resource details

MIME Type
application/json

Table 520. *POST /reference\_data/tables* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create



Table 520. POST /reference\_data/tables request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
element_type	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>key_name_types</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outer_key_label	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
key_name_types	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 521. POST /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## Scanner endpoints

Use the references for REST API V4 scanner endpoints.

### GET /scanner/profiles

Retrieves all of the currently created scan profiles.

No parameters are required and the following information should be retrieved for each scan profile:

- **scanProfileId**
- **scanProfileName**
- **description**
- **scanType**
- **scannerName**

Table 522. GET /scanner/profiles resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 523. GET /scanner/profiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

### Response Description

The list of scan profiles currently configured in QVM

### Response Sample

#### POST /scanner/profiles/create

Initiates a request to create a new scan profile.

The request takes one parameter - **createScanRequest**, which is just a POJO. To create the scan, you need to build up a JSON object that contains the Scan Profile name and ips to scan e.g. {'name': 'New Scan Profile', 'ips': ['10.100.85.135']}.

Table 524. POST /scanner/profiles/create resource details

MIME Type
text/plain

Table 525. POST /scanner/profiles/create request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 526. POST /scanner/profiles/create response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
419	9101	Occurs when a parameter is missing or invalid
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been created successfully or not.

## Response Sample

String

## POST /scanner/profiles/start

Initiates a request to start an existing scan profile.

The request takes one parameter - **scanProfileId**. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The **scanProfileId** is validated and an appropriate message returned.

Table 527. POST /scanner/profiles/start resource details

MIME Type
text/plain

Table 528. POST /scanner/profiles/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
scanProfileId	query	Required	String	text/plain	The unique id of the scan profile we want to start

Table 529. POST /scanner/profiles/start response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles

Retrieves all of the currently created scan profiles.

No parameters are required and the following information should be retrieved for each scan profile:

- **scanProfileId**
- **name**
- **description**
- **scanType**
- **scannerName**
- **schedule**
- **status**
- **progress**
- **endTime**
- **duration**

Table 530. GET /scanner/scanprofiles resource details

MIME Type
application/json

Table 531. GET /scanner/scanprofiles request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 531. GET /scanner/scanprofiles request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 532. GET /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
  }
]
```

```

        "scannerName": "String",
        "schedule": "String",
        "status": "String"
    }
]

```

## POST /scanner/scanprofiles

Initiates a request to create a new scanProfile.

The request takes one parameter - **createScanRequest**, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and hosts to scan e.g. `{'name': 'New Scan Profile', 'hosts': ['10.100.85.135']}`

Table 533. POST /scanner/scanprofiles resource details

MIME Type
text/plain

Table 534. POST /scanner/scanprofiles request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	Object	application/json	null	{ "description": "String", "hosts": [ "String" ], "name": "String" }

Table 535. POST /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan is created successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles/{profileid}

Retrieves a scan profile for a given Scan Profile ID.

The only parameter required is the Scan Profile ID. The following information about a scan profile is returned:

- **scanProfileId**
- **name**
- **description**
- **scanType**
- **scannerName**
- **schedule**
- **status**
- **progress**

- **endTime**
- **duration**

Table 536. GET /scanner/scanprofiles/{profileid} resource details

<b>MIME Type</b>
application/json

Table 537. GET /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we need to retrieve information for
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 538. GET /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
200		The scan profile was successfully returned
500	1030	Occurs when an attempt is made to list a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
  }
]
```

## POST /scanner/scanprofiles/{profileid}

Update a scan profile.

The Scan Profile ID is required. The following information on a scan profile can be updated: - name - description - ips eg {'name':'Updated Scan Profile', 'ips':['10.100.85.135']}

- **name**
- **description**
- **ips**

For example:

```
{'name':'Updated Scan Profile', 'ips':['10.100.85.135']}
```

Table 539. POST /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 540. POST /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile used to update



Table 541. *POST /scanner/scanprofiles/{profileid}* request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 542. *POST /scanner/scanprofiles/{profileid}* response codes

HTTP Response Code	Unique Code	Description
202		The scan profile was successfully updated
500	1030	Occurs when an attempt is made to update a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

A message to indicate whether the scan profile has updated or not.

## Response Sample

### **DELETE /scanner/scanprofiles/{profileid}**

Initiates a request to delete a scanProfile.

The request takes one parameter - the Scan Profile ID.

Table 543. *DELETE /scanner/scanprofiles/{profileid}* resource details

MIME Type
text/plain

Table 544. *DELETE /scanner/scanprofiles/{profileid}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	null

Table 545. *DELETE /scanner/scanprofiles/{profileid}* response codes

HTTP Response Code	Unique Code	Description
204		The scan has been successfully deleted
500	1030	Occurs when an attempt is made to delete a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been deleted successfully or not.

## Response Sample

String

### **POST /scanner/scanprofiles/{profileid}/start**

Initiates a request to start an already created scanProfile.

The request takes one parameter - **scanProfileId**, and one optional parameter - **ips**. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The **scanProfileId** is validated and an appropriate message returned.

Table 546. POST /scanner/scanprofiles/{profileid}/start resource details

<b>MIME Type</b>
text/plain

Table 547. POST /scanner/scanprofiles/{profileid}/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we want to start

Table 548. POST /scanner/scanprofiles/{profileid}/start request body details

Parameter	Data Type	MIME Type	Description	Sample
ips	JSON	application/json	null	null

Table 549. POST /scanner/scanprofiles/{profileid}/start response codes

HTTP Response Code	Unique Code	Description
202		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## SIEM endpoints

Use the references for REST API V4 SIEM endpoints.

### GET /siem/local\_destination\_addresses

Retrieve a list offense local destination addresses currently in the system.

Table 550. GET /siem/local\_destination\_addresses resource details

<b>MIME Type</b>
application/json

Table 551. GET /siem/local\_destination\_addresses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 552. GET /siem/local\_destination\_addresses response codes

HTTP Response Code	Unique Code	Description
200		The local destination address list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the local destination address list was being retrieved.

## Response Description

An array of local destination address objects. A local destination address object contains the following fields:

- **id** - Number - The ID of the destination address.
- **local\_destination\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the destination address.
- **network** - String - The network of the destination address.
- **offense\_ids** - Array of Numbers - List of offense IDs the destination address is part of.
- **source\_address\_ids** - Array of Numbers - List of source address IDs associated with the destination address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the destination address.

- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
[
  {
    "domain_id": 42,
    "event_flow_count": 42,
    "first_event_flow_seen": 42,
    "id": 42,
    "last_event_flow_seen": 42,
    "local_destination_ip": "String",
    "magnitude": 42,
    "network": "String",
    "offense_ids": [
      42
    ],
    "source_address_ids": [
      42
    ]
  }
]
```

## GET /siem/local\_destination\_addresses/{local\_destination\_address\_id}

Retrieve an offense local destination address.

Table 553. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} resource details

MIME Type
application/json

Table 554. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
local_destination_address_id	path	Required	Number (Integer)	text/plain	Required - The ID of the local destination address to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 555. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} response codes

HTTP Response Code	Unique Code	Description
200		The local destination was retrieved.
404	1002	No local destination address was found for the provided local_destination_address_id.
422	1005	A request parameter is not valid.

Table 555. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while the local destination address was being retrieved.

## Response Description

A local destination address object. A local destination address object contains the following fields:

- **id** - Number - The ID of the destination address.
- **local\_destination\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the destination address.
- **network** - String - The network of the destination address.
- **offense\_ids** - Array of Numbers - List of offense IDs the destination address is part of.
- **source\_address\_ids** - Array of Numbers - List of source address IDs associated with the destination address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the destination address.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
{
  "domain_id": 42,
  "event_flow_count": 42,
  "first_event_flow_seen": 42,
  "id": 42,
  "last_event_flow_seen": 42,
  "local_destination_ip": "String",
  "magnitude": 42,
  "network": "String",
  "offense_ids": [
    42
  ],
  "source_address_ids": [
    42
  ]
}
```

## GET /siem/offense\_closing\_reasons

Retrieve a list of all offense closing reasons.

Table 556. GET /siem/offense\_closing\_reasons resource details

MIME Type
application/json

Table 557. GET /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
include_reserved	query	Optional	Boolean	text/plain	Optional - If true, reserved closing reasons are included in the response. Defaults to false. Reserved closing reasons cannot be used to close an offense.
include_deleted	query	Optional	Boolean	text/plain	Optional - If true, deleted closing reasons are included in the response. Defaults to false. Deleted closing reasons cannot be used to close an offense.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 558. GET /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
200		The closing reasons list was retrieved.
500	1020	An error occurred while the closing reasons list was being retrieved.

## Response Description

An array of ClosingReason objects. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

## Response Sample

```
[
  {
    "id": 42,
    "is_deleted": true,
    "is_reserved": true,
    "text": "String"
  }
]
```

## POST /siem/offense\_closing\_reasons

Create an offense closing reason.

Table 559. POST /siem/offense\_closing\_reasons resource details

MIME Type
application/json

Table 560. POST /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
reason	query	Required	String	text/plain	Required - The text of the offense closing reason must be 5 - 60 characters in length.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 561. POST /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
201		The closing reason was created.
409	1004	The closing reason already exists.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create the closing reason.

## Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.

- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

### Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

### GET /siem/offense\_closing\_reasons/{closing\_reason\_id}

Retrieve an offense closing reason.

Table 562. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} resource details

MIME Type
application/json

Table 563. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
closing_reason_id	path	Required	Number (Integer)	text/plain	Required - The closing reason ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 564. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} response codes

HTTP Response Code	Unique Code	Description
200		The closing reason was retrieved.
404	1002	No closing reason was found for the provided closing_reason_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the closing reason.

### Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.



## Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

## GET /siem/offenses

Retrieve a list of offenses currently in the system.

Table 565. GET /siem/offenses resource details

MIME Type
application/json

Table 566. GET /siem/offenses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 567. GET /siem/offenses response codes

HTTP Response Code	Unique Code	Description
200		The offense list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the offense list was being retrieved.

## Response Description

An array of Offense objects. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense. Filtering is not supported on this field.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense. Filtering is not supported on this field.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense. Filtering is not supported on this field.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.

- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED". The following operators are not supported when you filter on this field: "<", ">", "<=", ">=", "BETWEEN".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers -The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 568. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
[{"credibility": 42,
  "source_address_ids": [42],
  "remote_destination_count": 42,
  "local_destination_address_ids": [42],
  "assigned_to": "String",
  "local_destination_count": 42,
  "source_count": 42,
  "start_time": 42,
  "id": 42,
  "destination_networks": ["String"],
  "inactive": true,
  "protected": true,
  "policy_category_count": 42,
  "description": "String",
  "category_count": 42,
  "domain_id": 42,
```

```

"relevance": 42,
"device_count": 42,
"security_category_count": 42,
"flow_count": 42,
"event_count": 42,
"offense_source": "String",
"status": "String <one of: OPEN, HIDDEN, CLOSED>",
"magnitude": 42,
"severity": 42,
"username_count": 42,
"closing_user": "String",
"follow_up": true,
"closing_reason_id": 42,
"close_time": 42,
"source_network": "String",
"last_updated_time": 42,
"categories": ["String"],
"offense_type": 42}]

```

## GET /siem/offenses/{offense\_id}

Retrieve an offense structure that describes properties of an offense

Table 569. GET /siem/offenses/{offense\_id} resource details

MIME Type
application/json

Table 570. GET /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 571. GET /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense was being retrieved.

## Response Description

An Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.

- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers -The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 572. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
  "close_time": 42,
  "closing_reason_id": 42,
  "closing_user": "String",
  "credibility": 42,
  "description": "String",
  "destination_networks": [
    "String"
  ],
  "device_count": 42,
  "domain_id": 42,
  "event_count": 42,
  "flow_count": 42,
  "follow_up": true,
}
```

```

    "id": 42,
    "inactive": true,
    "last_updated_time": 42,
    "local_destination_address_ids": [
        42
    ],
    "local_destination_count": 42,
    "magnitude": 42,
    "offense_source": "String",
    "offense_type": 42,
    "policy_category_count": 42,
    "protected": true,
    "relevance": 42,
    "remote_destination_count": 42,
    "security_category_count": 42,
    "severity": 42,
    "source_address_ids": [
        42
    ],
    "source_count": 42,
    "source_network": "String",
    "start_time": 42,
    "status": "String <one of: OPEN, HIDDEN, CLOSED>",
    "username_count": 42
}

```

## POST /siem/offenses/{offense\_id}

Update an offense.

Table 573. POST /siem/offenses/{offense\_id} resource details

MIME Type
application/json

Table 574. POST /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The ID of the offense to update.
protected	query	Optional	Boolean	text/plain	Optional - Set to true to protect the offense.
follow_up	query	Optional	Boolean	text/plain	Optional - Set to true to set the follow up flag on the offense.
status	query	Optional	String	text/plain	Optional - The new status for the offense. Set to one of: OPEN, HIDDEN, CLOSED. When the status of an offense is being set to CLOSED, a valid closing_reason_id must be provided. To hide an offense, use the HIDDEN status. To show a previously hidden offense, use the OPEN status.
closing_reason_id	query	Optional	Number (Integer)	text/plain	Optional - The ID of a closing reason. You must provide a valid closing_reason_id when you close an offense.

Table 574. POST /siem/offenses/{offense\_id} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
assigned_to	query	Optional	String	text/plain	Optional - A user to assign the offense to.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 575. POST /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was updated.
403	1009	User does not have the required capability to assign an offense.
404	1002	No offense was found for the provided offense_id.
409	1008	Request cannot be completed due to the state of the offense.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense was being updated.

## Response Description

An updated Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.



- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers - The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 576. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port

Table 576. Offense Type Codes (continued)

Code	Offense Type
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

### Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
  "close_time": 42,
  "closing_reason_id": 42,
  "closing_user": "String",
  "credibility": 42,
  "description": "String",
  "destination_networks": [
    "String"
  ],
  "device_count": 42,
  "domain_id": 42,
  "event_count": 42,
  "flow_count": 42,
  "follow_up": true,
  "id": 42,
  "inactive": true,
  "last_updated_time": 42,
  "local_destination_address_ids": [
    42
  ],
  "local_destination_count": 42,
  "magnitude": 42,
  "offense_source": "String",
  "offense_type": 42,
  "policy_category_count": 42,
  "protected": true,
  "relevance": 42,
  "remote_destination_count": 42,
  "security_category_count": 42,
  "severity": 42,
  "source_address_ids": [
    42
  ],
  "source_count": 42,
  "source_network": "String",
  "start_time": 42,
  "status": "String <one of: OPEN, HIDDEN, CLOSED>",
  "username_count": 42
}
```

## GET /siem/offenses/{offense\_id}/notes

Retrieve a list of notes for an offense.

Table 577. GET /siem/offenses/{offense\_id}/notes resource details

MIME Type
application/json

Table 578. GET /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the notes for.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 579. GET /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
200		The note list was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the note list was being retrieved.

### Response Description

An array of Note objects. A Note object contains the following fields:

- **id** - Number - The ID of the note.

- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

### Response Sample

```
[
  {
    "create_time": 42,
    "id": 42,
    "note_text": "String",
    "username": "String"
  }
]
```

### POST /siem/offenses/{offense\_id}/notes

Create a note on an offense.

Table 580. POST /siem/offenses/{offense\_id}/notes resource details

MIME Type
application/json

Table 581. POST /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to add the note to.
note_text	query	Required	String	text/plain	Required - The note text.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 582. POST /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
201		The note was created.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create the note.

## Response Description

The Note object that was created. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## GET /siem/offenses/{offense\_id}/notes/{note\_id}

Retrieve a note for an offense.

Table 583. GET /siem/offenses/{offense\_id}/notes/{note\_id} resource details

MIME Type
application/json

Table 584. GET /siem/offenses/{offense\_id}/notes/{note\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the note from.
note_id	path	Required	Number (Integer)	text/plain	Required - The note ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 585. GET /siem/offenses/{offense\_id}/notes/{note\_id} response codes

HTTP Response Code	Unique Code	Description
200		The note was retrieved.
404	1002	No offense was found for the provided offense_id.
404	1003	No note was found for the provided note_id.
422	1005	A request parameter is not valid.

Table 585. GET /siem/offenses/{offense\_id}/notes/{note\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to retrieve the note.

## Response Description

The Note object for the note ID. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## GET /siem/source\_addresses

Retrieve a list offense source addresses currently in the system.

Table 586. GET /siem/source\_addresses resource details

MIME Type
application/json

Table 587. GET /siem/source\_addresses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 587. GET /siem/source\_addresses request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 588. GET /siem/source\_addresses response codes

HTTP Response Code	Unique Code	Description
200		The source address list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the source address list was being retrieved.

## Response Description

An array of source address objects. A source address object contains the following fields:

- **id** - Number - The ID of the source.
- **source\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the source address.
- **network** - String - The network of the source address.
- **offense\_ids** - Array of Numbers - List of offense IDs the source is part of.
- **local\_destination\_address\_ids** - Array of Numbers - List of local destination address IDs associated with the source address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the source.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
[
  {
    "domain_id": 42,
    "event_flow_count": 42,
    "first_event_flow_seen": 42,
    "id": 42,
    "last_event_flow_seen": 42,
    "local_destination_address_ids": [
      42
    ],
    "magnitude": 42,
    "network": "String",
    "offense_ids": [
```

```

    42
  ],
  "source_ip": "String"
}
]

```

## GET /siem/source\_addresses/{source\_address\_id}

Retrieve an offense source address.

Table 589. GET /siem/source\_addresses/{source\_address\_id} resource details

<b>MIME Type</b>
application/json

Table 590. GET /siem/source\_addresses/{source\_address\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
source_address_id	path	Required	Number (Integer)	text/plain	Required - The ID of the source address to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 591. GET /siem/source\_addresses/{source\_address\_id} response codes

HTTP Response Code	Unique Code	Description
200		The source address was retrieved.
404	1002	No source address was found for the provided source_address_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the source address was being retrieved.

## Response Description

A source address object. A source address object contains the following fields:

- **id** - Number - The ID of the source.
- **source\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the source address.
- **network** - String - The network of the source address.
- **offense\_ids** - Array of Numbers - List of offense IDs the source is part of.
- **local\_destination\_address\_ids** - Array of Numbers - List of local destination address IDs associated with the source address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the source.



- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

### Response Sample

```
{
  "domain_id": 42,
  "event_flow_count": 42,
  "first_event_flow_seen": 42,
  "id": 42,
  "last_event_flow_seen": 42,
  "local_destination_address_ids": [
    42
  ],
  "magnitude": 42,
  "network": "String",
  "offense_ids": [
    42
  ],
  "source_ip": "String"
}
```

---

## REST API V3.1 References

Each API reference provides information about the parameters, mime type, stability, and responses for each endpoint.

### Ariel endpoints

Use the references for REST API V3.1 ariel endpoints.

#### **GET /ariel/databases DEPRECATED**

Retrieve Ariel database names

Retrieve a list of available Ariel databases.

*Table 592. GET /ariel/databases resource details*

<b>MIME Type</b>
application/json

*Table 593. GET /ariel/databases request parameter details*

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 593. GET /ariel/databases request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 594. GET /ariel/databases response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of Ariel databases.

## Response Description

The names of the available Ariel databases.

## Response Sample

```
[
  "String"
]
```

## GET /ariel/databases/{database\_name} DEPRECATED

Retrieve the columns defined for a specific Ariel database.

Retrieve the columns that are defined for the specified Ariel database. This is the set of columns that can be explicitly named in the column list of a SELECT query.

Table 595. GET /ariel/databases/{database\_name} resource details

MIME Type
application/json

Table 596. GET /ariel/databases/{database\_name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
database_name	path	Required	String	text/plain	Required. The name of the Ariel database that contains the columns that you want to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 596. GET /ariel/databases/{database\_name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 597. GET /ariel/databases/{database\_name} response codes

HTTP Response Code	Unique Code	Description
200		The database columns were retrieved.
404	1002	The database does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the database columns.

## Response Description

A list of columns that are defined for the specified database. Multiple properties of each column are returned. For example, the column name or an indication that the column is indexable.

## Response Sample

```
{
  "columns": [
    {
      "argument_type": "String",
      "indexable": true,
      "name": "String"
    }
  ]
}
```

## GET /ariel/searches DEPRECATED

Retrieve Ariel search\_ids.

Retrieve the list of Ariel searches. This includes search\_ids for completed and active searches.

Table 598. GET /ariel/searches resource details

MIME Type
application/json

Table 599. GET /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 600. GET /ariel/searches response codes

HTTP Response Code	Unique Code	Description
200		The search list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of searches.

## Response Description

A list of search IDs.

## Response Sample

```
[
  "String"
]
```

## POST /ariel/searches DEPRECATED

Create a new asynchronous Ariel search

Create an Ariel search based on Ariel Query Language (AQL) query expressions. A search\_id is returned with the search results. Searches are executed asynchronously. In subsequent API calls, you can use this search\_id to determine the status of the search and retrieve the results.

This endpoint only accepts SELECT and RUN query expressions.

Queries are applied to the range of data in a time interval. The default time interval is the last 60 seconds. You can specify an alternate time interval in your query expression. For more information, see the AQL Reference Guide.

Table 601. POST /ariel/searches resource details

MIME Type
application/json

Table 602. POST /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
query_expression	query	Required	String	text/plain	Required. The AQL query to execute.
search_id	query	Optional	String	text/plain	Optional. A custom search_id value for the new search to replace the system generated search_id. The search_id must be unique and is only used for SELECT query expressions. The search_id can only contain numbers, letters, dashes, and underscores.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 603. POST /ariel/searches response codes

HTTP Response Code	Unique Code	Description
201		An Ariel search was successfully created.
409	1004	The search could not be created. The search_id provided is already in use. Use a unique search_id.
422	2000	The query_expression contains invalid AQL syntax.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create a new search.

## Response Description

Information about the specified search, including the search\_id. Use the search\_id to access or manipulate the search with the other API endpoints.

If the search has the same search criteria as an existing search, the response message returns a reference to the original search\_id and does not create a new search.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
}
```

```

    "processed_record_count": 42,
    "progress": 42,
    "query_execution_time": 42,
    "record_count": 42,
    "save_results": true,
    "search_id": "String",
    "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
  }

```

## GET /ariel/searches/{search\_id} DEPRECATED

Retrieve information about an Ariel search

Retrieve status information for a search, based on the search\_id parameter. The same informational fields are returned regardless of whether the search is in progress or is complete.

Table 604. GET /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 605. GET /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The identifier for an Ariel search.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 606. GET /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search information was retrieved.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search information.

## Response Description

Information about the specified search, including the search status.

## Response Sample

```

{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,

```

```

"cursor_id": "String",
"data_file_count": 42,
"data_total_size": 42,
"desired_retention_time_msec": 42,
"error_messages": [
  {
    "code": "String",
    "contexts": [
      "String"
    ],
    "message": "String",
    "severity": "String <one of: INFO, WARN, ERROR>"
  }
],
"index_file_count": 42,
"index_total_size": 42,
"processed_record_count": 42,
"progress": 42,
"query_execution_time": 42,
"record_count": 42,
"save_results": true,
"search_id": "String",
"status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}

```

## POST /ariel/searches/{search\_id} DEPRECATED

Update an Ariel search.

Update details for an Ariel search. You can update searches in the following ways:

- To cancel an active search, set the **status** parameter to CANCELED. This stops the search and keeps any search results that were collected before the search was canceled.
- The results for a completed search can be saved by setting the **save\_results** parameter to true. This ensures that the search is not automatically removed when it expires in accordance with the retention policy.

The Ariel server uses an internal retention policy to manage available disk space. Searches might be deleted automatically, according to the settings of the retention policy. Searches with saved results are not automatically reclaimed by the server and are therefore retained. A search can be explicitly deleted by using the DELETE /searches/{search\_id} endpoint.

Note: Saving too many search results might result in insufficient disk space to process new searches.

Table 607. POST /ariel/searches/{search\_id} resource details

<b>MIME Type</b>
application/json

Table 608. POST /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The ID of the search to update.

Table 608. POST /ariel/searches/{search\_id} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
save_results	query	Optional	String	text/plain	Optional. The only accepted value is true. If this value is provided, the search results will not be deleted by the search expiration removal process.
status	query	Optional	String	text/plain	Optional. The only accepted value is CANCELED. If this value is provided, the search will be canceled.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 609. POST /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search was updated.
404	1002	The search does not exist.
409	1008	The current status of the search prevented the search results from being saved.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to update the search.

## Response Description

Information about the specified search that was updated.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
```



```

        "String"
    ],
    "message": "String",
    "severity": "String <one of: INFO, WARN, ERROR>"
  }
],
"index_file_count": 42,
"index_total_size": 42,
"processed_record_count": 42,
"progress": 42,
"query_execution_time": 42,
"record_count": 42,
"save_results": true,
"search_id": "String",
"status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}

```

## DELETE /ariel/searches/{search\_id} DEPRECATED

Delete an Ariel search.

Deletes an Ariel search. This discards collected results and stops the search if it in progress. This search is deleted regardless of whether the results were saved.

Table 610. DELETE /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 611. DELETE /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The search_id of the search to delete.

Table 612. DELETE /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
204		The search was deleted.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to delete the search.

## Response Description

There is no response body for a successfully deleted Ariel Search.

## Response Sample

```

{
  "error_messages": [
    {
      "code": "String <one of: ERROR_FILE_ACCESS,
        ERROR_CURSOR_CREATE,
        ERROR_CURSOR_CREATE_EXISTS,
        WARN_MAX_RECORDS,
        WARN_MAX_COLLECTED_RECORDS,
        ERROR_INVALID_CURSOR,

```

```

        ERROR_PROTECT_CURSOR,
        ERROR_SERVER_IO,
        WARN_INTERRUPT,
        ERROR_READ_TIMEOUT,
        ERROR_INVALID_QUERY_PARAMS,
        WARN_QUERY_TIME_LIMIT,
        ERROR_GENERAL_FAILURE,
        ERROR_FILE_RUNTIME_EXCEPTION,
        ERROR_INVALID_QUERY,
        WARN_CANCEL,
        INFO_INVALID_SORTING,
        ERROR_FETCH,
        WARN_SHARING_VIOLATION,
        WARN_INCOMPLETE_RESULT,
        ERROR_QUERY_EXPIRED,
        INFO_MAINTENANCE,
        ERROR_FUNCTION_ERROR,
        ERROR_COULD_NOT_CONNECT,
        ERROR_RB_COMMUNICATION,
        ERROR_RB_SOURCE_DATABLOCK_SEND,
        ERROR_RB_DESTINATION_DATABLOCK_RECEIVE,
        NEXUS_ERROR>",
    "contexts": [
        "String"
    ],
    "message": "String",
    "severity": "String <one of: INFO, WARN, ERROR>"
}
]
}

```

## GET /ariel/searches/{search\_id}/results DEPRECATED

Retrieves search results in the requested format.

Retrieve the results of the Ariel search that is identified by the search\_id. The Accepts request header indicates the format of the result. The format can be JSON, CSV, XML, or tabular text.

By default, all query result records are returned. To restrict the results to a contiguous subset of the records, you can supply a Range header to specify the inclusive range of records to be returned.

This end-point works with query results that are generated by AQL query expressions. This endpoint might not work as expected for results that are generated by other means. Search results might not be retrievable for searches that are created on the Console.

The response samples are for the following query: Select sourceIP, destinationIP from events.

Table 613. GET /ariel/searches/{search\_id}/results resource details

MIME Type
application/json application/csv text/table application/xml

Table 614. GET /ariel/searches/{search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	The ID of the search criteria for the returned results.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 615. GET /ariel/searches/{search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The search results were retrieved.
404	1002	The search does not exist.
404	1003	Search results not found. The search is still in progress.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search results.

## Response Description

The search results for the specified search\_id. The format that is used to encapsulate the data depends on the format specified in the Accept header for this request.

## Response Sample

```
{
  "events": [
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    },
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    }
  ]
}
```

## Asset model endpoints

Use the references for REST API V3.1 Asset Model endpoints.

## GET /asset\_model/assets DEPRECATED

List all assets found in the model.

Table 616. GET /asset\_model/assets resource details

<b>MIME Type</b>
application/json

Table 617. GET /asset\_model/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 618. GET /asset\_model/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
500	1020	The server encountered an error while trying to retrieve the assets.

### Response Description

List of assets retrieved using the associated asset saved search.

### Response Sample

```
[{"id": 42,
  "domain_id": 42,
  "interfaces": [{"first_seen_scanner": 42,
                  "id": 42,
                  "first_seen_profiler": 42,
                  "created": 42,
                  "last_seen_profiler": 42,
```

```

        "last_seen_scanner": 42,
        "mac_address": "String",
        "ip_addresses": [{"first_seen_scanner": 42,
                           "id": 42,
                           "first_seen_profiler": 42,
                           "created": 42,
                           "network_id": 42,
                           "value": "String",
                           "last_seen_profiler": 42,
                           "last_seen_scanner": 42,
                           "type": "String"}]
    },
    "properties": [{"id": 42,
                    "name": "String",
                    "value": "String",
                    "last_reported": 42,
                    "type_id": 42,
                    "last_reported_by": "String"}]
}]

```

## POST /asset\_model/assets/{asset\_id} DEPRECATED

Update an asset with several pertinent pieces of information.

The **asset\_id** tag is mandatory, and is the unique identifier for an asset. This field is available through the `/asset_model/assets` or `/asset_model/saved_searches/{saved_search_id}/results` query. To update properties, the property type id which is available through the `/asset_model/properties` query should be provided along with the new value. See the sample provided demonstrating an example asset update.

Table 619. POST /asset\_model/assets/{asset\_id} resource details

<b>MIME Type</b>
text/plain

Table 620. POST /asset\_model/assets/{asset\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
asset_id	path	Required	String	text/plain	Unique identifier of the asset to update.

Table 621. POST /asset\_model/assets/{asset\_id} request body details

Parameter	Data Type	MIME Type	Description	Sample
asset	JSON	application/json	JSON representation of an asset.	{ "properties": [ { "type_id": 1001, "value": "given name value" }, { "type_id": 1002, "value": "unified name value" } ] }

Table 622. POST /asset\_model/assets/{asset\_id} response codes

HTTP Response Code	Unique Code	Description
202		The request to update the asset was successful. The update will take place when the asset profile application receives the request.
422	1005	One or more of the requested property updates were invalid.

Table 622. *POST /asset\_model/assets/{asset\_id}* response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	The server encountered an error registering the update with the asset profile application.

## Response Description

Information about the asset that was updated.

## Response Sample

String

## GET /asset\_model/properties DEPRECATED

Get a list of available asset property types that can be used.

Get a list of available asset property types that can be used or applied against the */asset\_model/assets* endpoint.

Table 623. *GET /asset\_model/properties* resource details

MIME Type
application/json

Table 624. *GET /asset\_model/properties* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 625. GET /asset\_model/properties response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of asset property types completed successfully.
500	1020	An error occurred while trying to retrieve the list of asset property types.

## Response Description

List of asset properties. Per asset property type: id and name that make up this asset property type.

## Response Sample

```
[
  {
    "custom": true,
    "data_type": "String",
    "display": true,
    "id": 42,
    "name": "String",
    "state": 42
  }
]
```

## GET /asset\_model/saved\_searches DEPRECATED

Get a list of saved searches that can be used.

Get a list of saved searches that can be used or applied against the `/asset_model/saved_searches/{saved_search_id}/results` query.

Table 626. GET /asset\_model/saved\_searches resource details

MIME Type
application/json

Table 627. GET /asset\_model/saved\_searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 627. GET /asset\_model/saved\_searches request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 628. GET /asset\_model/saved\_searches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully.
500	1020	The server encountered an error while trying to retrieve the list of saved searches.

## Response Description

List of saved searches. Per saved search: id, name and list of filters that make up this saved search

## Response Sample

```
[
  {
    "columns": [
      {
        "name": "String",
        "type": "String"
      }
    ],
    "description": "String",
    "filters": [
      {
        "operator": "String",
        "parameter": "String",
        "value": "String"
      }
    ],
    "id": 42,
    "name": "String"
  }
]
```



## GET /asset\_model/saved\_searches/{saved\_search\_id}/results DEPRECATED

Retrieves a list of assets based on the results of an asset saved search.

Retrieves a list of assets based on the results of an asset saved search.

Table 629. GET /asset\_model/saved\_searches/{saved\_search\_id}/results resource details

MIME Type
application/json

Table 630. GET /asset\_model/saved\_searches/{saved\_search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
saved_search_id	path	Required	String	text/plain	Unique identifier of the saved search used to retrieve assets.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 631. GET /asset\_model/saved\_searches/{saved\_search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
422	1005	The unique identifier of the saved search provided was invalid.
500	1003	The server encountered an error executing the saved search.

### Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[
  {
    "domain_id": 42,
    "id": 42,
    "interfaces": [
      {
        "created": 42,
        "first_seen_profiler": 42,
        "first_seen_scanner": 42,
        "id": 42,
        "ip_addresses": [
          {
            "created": 42,
            "first_seen_profiler": 42,
            "first_seen_scanner": 42,
            "id": 42,
            "last_seen_profiler": 42,
            "last_seen_scanner": 42,
            "network_id": 42,
            "type": "String",
            "value": "String"
          }
        ],
        "last_seen_profiler": 42,
        "last_seen_scanner": 42,
        "mac_address": "String"
      }
    ],
    "properties": [
      {
        "id": 42,
        "last_reported": 42,
        "last_reported_by": "String",
        "name": "String",
        "type_id": 42,
        "value": "String"
      }
    ]
  }
]
```

## Authentication endpoints

Use the references for REST API V3.1 authentication endpoints.

### POST /auth/logout DEPRECATED

Invoke this method as an authorized user and your session will be invalidated.

Table 632. POST /auth/logout resource details

MIME Type
text/plain

There are no parameters for this endpoint.

Table 633. POST /auth/logout response codes

HTTP Response Code	Unique Code	Description
200		The session was invalidated.

## Response Description

Returns true. Throws exception upon failure.

## Response Sample

```
true
```

## Help endpoints

Use the references for REST API V3.1 Help endpoints.

### GET /help/capabilities DEPRECATED

List all QRadar API capabilities

List the QRadar API capabilities. The response will contain all available RESTful resources We allow every authenticated user to access this method, but restrict the output based on their user capabilities

Table 634. GET /help/capabilities resource details

<b>MIME Type</b>
application/json

Table 635. GET /help/capabilities request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
categories	query	Optional	Array<String>	application/json	Optional - Restrict your search to this list of capabilities
paths	query	Optional	Array<String>	application/json	Optional - Restrict your search to these paths only
httpMethods	query	Optional	Array<String>	application/json	Optional - Restrict your search to these HTTP methods
version	query	Optional	String	text/plain	Optional - Restrict your search to this version (or below)
showExperimental	query	Optional	Boolean	text/plain	Optional - If true, we include experimental endpoints (default is true)
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 636. GET /help/capabilities response codes

HTTP Response Code	Unique Code	Description
200		The API capabilities list was retrieved.
422	1001	Invalid input
422	1002	Our internal mapping has an unexpected structure or contains an invalid element value

Table 636. GET /help/capabilities response codes (continued)

HTTP Response Code	Unique Code	Description
500	1003	A generic error has occurred while retrieving our capabilities

## Response Description

Endpoints you are able to access, mapped against versions they belong to. If full content is not requested, values will be null.

## Response Sample

```
{
  "categories": [
    {
      "apis": [
        {
          "httpMethod": "String <one of: OPTIONS,
                                GET,
                                HEAD,
                                POST,
                                PUT,
                                DELETE,
                                TRACE,
                                CONNECT,
                                PATCH>",
          "operations": [
            {
              "additionalFiltering": true,
              "deprecated": true,
              "description": "String",
              "errorResponses": [
                {
                  "code": 42,
                  "description": "String",
                  "uniqueCode": 42
                }
              ],
              "httpMethod": "String",
              "lastSupportedVersion": "String",
              "parameters": [
                {
                  "allowMultiple": true,
                  "defaultValue": "String",
                  "description": "String",
                  "name": "String",
                  "pathIndex": 42,
                  "required": true,
                  "source": "String",
                  "supportedContentTypes": [
                    {
                      "dataType": "String",
                      "mimeType": "String",
                      "sample": "String"
                    }
                  ]
                }
              ]
            }
          ],
          "removalTarget": "String",
          "removed": true,
          "responseClass": "String",
          "responseDescription": {
            "description": "String",

```

```

        "properties": [
            {
                "description": "String",
                "name": "String"
            }
        ],
    },
    "successResponses": [
        {
            "code": 42,
            "description": "String"
        }
    ],
    "summary": "String",
    "supportedContentTypes": [
        {
            "dataType": "String",
            "mimeType": "String",
            "sample": "String"
        }
    ],
    "version": "String",
    "visibility": "String"
    },
    "path": "String"
    },
    "path": "String"
    },
    "path": "String"
}

```

## QRadar Vulnerability Manager endpoints

Use the references for REST API V3.1 QRadar Vulnerability Manager endpoints.

### GET /qvm/assets DEPRECATED

List the assets with discovered vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 637. GET /qvm/assets resource details

MIME Type
application/json

Table 638. GET /qvm/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 639. GET /qvm/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by asset completed successfully
420	9101	Invalid search parameters, search cannot be performed

### Response Description

list of assets data

### Response Sample

#### GET /qvm/filters DEPRECATED

Get a list of the allowable filters that can be used or applied against /qvm endpoints.

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 640. GET /qvm/filters resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 641. GET /qvm/filters response codes

HTTP Response Code	Unique Code	Description
200		The search executed successfully
420	9102	An error occurred while executing the search

### Response Description

list of Filters.

### Response Sample

#### GET /qvm/network DEPRECATED

List the networks present in the asset model with vulnerabilities present. The response will contain all available RESTful resources

Table 642. GET /qvm/network resource details

MIME Type
application/json

Table 643. GET /qvm/network request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 644. GET /qvm/network response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by network completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of network related data

## Response Sample

### GET /qvm/openservices DEPRECATED

List the openservices present in the asset model with vulnerabilities present. The response will contain all available RESTful resources

Table 645. GET /qvm/openservices resource details

MIME Type
application/json

Table 646. GET /qvm/openservices request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 647. GET /qvm/openservices response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by open service completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of open services related data

## Response Sample

### GET /qvm/savedsearches DEPRECATED

Get a list of saved searches that can be applied against /qvm endpoints.

A list of saved searches that can be applied against the following endpoints:

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 648. GET /qvm/savedsearches resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 649. GET /qvm/savedsearches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully
420	9103	An error occurred while trying to retrieve the list of saved searches

## Response Description

list of saved searches. Per saved search: id, name and list fo filters that make up this saved search

## Response Sample

### POST /qvm/tickets/assign DEPRECATED

Update the remediation ticket for the assigned vulnerability

Table 650. POST /qvm/tickets/assign resource details

<b>MIME Type</b>
application/json



Table 651. POST /qvm/tickets/assign request body details

Parameter	Data Type	MIME Type	Description	Sample
ticket	JSON	application/json	<p>'ticketId': required.</p> <p>'priority' one of required : Critical, Major, Minor, Warning, Informational.</p> <p>'status' one of required : Opened, Fixed, Re-Opened, Closed .</p> <p>'dueDate' Optional : yyyy-MM-dd HH:mm:ss.</p> <p>'assignedUser' required : valid QRadar user account name or a valid email.</p> <p>'comment' Optional : text.</p> <p>'commentUser' Optional : valid QRadar user account name, if not included will default current API user.</p>	[ { "ticketId":"1000", "status":"Opened", "priority":"Critical", "dueDate":"2015-01-04 12:00:00", "assignedUser":"admin", "comment":"testComment", "commentUser":"admin" } ]

Table 652. POST /qvm/tickets/assign response codes

HTTP Response Code	Unique Code	Description
200		The request to assign a ticket completed successfully
420	9104	An error occurred while trying to assign a ticket due to invalid arguments

## Response Description

success message if update succeed

## Response Sample

### GET /qvm/vulninstances DEPRECATED

List the Vulnerability Instances present in the asset model. The response will contain all available RESTful resources

Table 653. GET /qvm/vulninstances resource details

MIME Type
application/json

Table 654. GET /qvm/vulninstances request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	<p>List of JSON objects for application of bespoke query search dataset filter.</p> <p>Format</p> <p>[{"parameter":"&lt;value&gt;", "operator":"&lt;value&gt;", "value":"&lt;value&gt;"}] e.g.</p> <p>[{"parameter":"IPv4 Address", "operator":"Equals", "value":"10.100.85.111"}]</p>

Table 655. GET /qvm/vulninstances response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by instance completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability instance data

## Response Sample

### GET /qvm/vulns DEPRECATED

List the Vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 656. GET /qvm/vulns resource details

MIME Type
application/json

Table 657. GET /qvm/vulns request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 658. GET /qvm/vulns response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability data

## Response Sample

## Reference data endpoints

Use the references for REST API V3.1 reference data endpoints.

## GET /reference\_data/map\_of\_sets DEPRECATED

Retrieve a list of all reference map of sets.

Table 659. GET /reference\_data/map\_of\_sets resource details

<b>MIME Type</b>
application/json

Table 660. GET /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 661. GET /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

### Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

### Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
```

```

    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]

```

## POST /reference\_data/map\_of\_sets DEPRECATED

Create a new reference map of sets.

Table 662. POST /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 663. POST /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 663. POST /reference\_data/map\_of\_sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 664. POST /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/map\_of\_sets/{name} DEPRECATED

Return the reference map of sets identified by name.

Return the reference map of sets identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 665. GET /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 666. GET /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 667. GET /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map of sets

## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": [
      {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    ]
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
}
```

```

"name": "String",
"number_of_elements": 42,
"time_to_live": "String",
"timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"value_label": "String"
}

```

## POST /reference\_data/map\_of\_sets/{name} DEPRECATED

Add or update an element in a reference map of sets.

Table 668. POST /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 669. POST /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 670. POST /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist

Table 670. *POST /reference\_data/map\_of\_sets/{name}* response codes (continued)

HTTP Response Code	Unique Code	Description
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map of sets

## Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name} DEPRECATED

Remove a map of sets or purge its contents.

Table 671. *DELETE /reference\_data/map\_of\_sets/{name}* resource details

MIME Type
application/json

Table 672. *DELETE /reference\_data/map\_of\_sets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.



Table 672. DELETE /reference\_data/map\_of\_sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 673. DELETE /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map of sets does not exist
409	1004	The reference map of sets could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

## Response Description

If the reference map of sets was removed nothing is returned, otherwise information about the reference map of sets that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name}/{key} DEPRECATED

Remove a value from a reference map of sets.

Table 674. DELETE /reference\_data/map\_of\_sets/{name}/{key} resource details

MIME Type
application/json

Table 675. DELETE /reference\_data/map\_of\_sets/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 676. DELETE /reference\_data/map\_of\_sets/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

## Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
```

```

"time_to_live": "String",
"timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"value_label": "String"
}

```

## GET /reference\_data/maps DEPRECATED

Retrieve a list of all reference maps.

Table 677. GET /reference\_data/maps resource details

<b>MIME Type</b>
application/json

Table 678. GET /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 679. GET /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

## Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## POST /reference\_data/maps DEPRECATED

Create a new reference map.

Table 680. POST /reference\_data/maps resource details

MIME Type
application/json

Table 681. POST /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 681. *POST /reference\_data/maps request parameter details (continued)*

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 682. *POST /reference\_data/maps response codes*

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps/{name} DEPRECATED

Retrieve the reference map identified by name.

Retrieve the reference map identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 683. *GET /reference\_data/maps/{name} resource details*

MIME Type
application/json

Table 684. GET /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 685. GET /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",

```

```

        "value": "String"
    }
},
"element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
"key_label": "String",
"name": "String",
"number_of_elements": 42,
"time_to_live": "String",
"timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"value_label": "String"
}

```

## POST /reference\_data/maps/{name} DEPRECATED

Add or update an element in a reference map.

Table 686. POST /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 687. POST /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 688. *POST /reference\_data/maps/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/maps/{name} DEPRECATED

Remove a reference map or purge its contents.

Table 689. *DELETE /reference\_data/maps/{name}* resource details

MIME Type
application/json

Table 690. *DELETE /reference\_data/maps/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.



Table 690. DELETE /reference\_data/maps/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 691. DELETE /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map does not exist
409	1004	The reference map could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

## Response Description

If the reference map was removed nothing is returned, otherwise information about the reference map that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/maps/{name}/{key} DEPRECATED

Remove a value from a reference map.

Table 692. DELETE /reference\_data/maps/{name}/{key} resource details

MIME Type
application/json

Table 693. DELETE /reference\_data/maps/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 694. DELETE /reference\_data/maps/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

## Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/sets DEPRECATED

Retrieve a list of all reference sets.

Table 695. GET /reference\_data/sets resource details

<b>MIME Type</b>
application/json

Table 696. GET /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 697. GET /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

### Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

### Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "number_of_elements": 42,
```

```

    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]

```

## POST /reference\_data/sets DEPRECATED

Create a new reference set.

Table 698. POST /reference\_data/sets resource details

MIME Type
application/json

Table 699. POST /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 700. *POST /reference\_data/sets* response codes

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/sets/{name} DEPRECATED

Retrieve the reference set identified by name.

Retrieve the reference set identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 701. *GET /reference\_data/sets/{name}* resource details

MIME Type
application/json

Table 702. *GET /reference\_data/sets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 702. GET /reference\_data/sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 703. GET /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": [
    {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  ],
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/{name} DEPRECATED

Add or update an element in a reference set.

Table 704. POST /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 705. POST /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 706. POST /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update an element in the reference set

## Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
```

```

    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## DELETE /reference\_data/sets/{name} DEPRECATED

Remove a reference set or purge its contents.

Table 707. DELETE /reference\_data/sets/{name} resource details

<b>MIME Type</b>
application/json

Table 708. DELETE /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 709. DELETE /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had its contents purged
204		The reference set has been removed
404	1002	The reference set does not exist
409	1004	The reference set could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference set



## Response Description

If the reference set was removed nothing is returned, otherwise information about the reference set that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/sets/{name}/{value} DEPRECATED

Remove a value from a reference set.

Table 710. DELETE /reference\_data/sets/{name}/{value} resource details

MIME Type
application/json

Table 711. DELETE /reference\_data/sets/{name}/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 712. DELETE /reference\_data/sets/{name}/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist

Table 712. DELETE /reference\_data/sets/{name}/{value} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had an value removed. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/bulk\_load/{name} DEPRECATED

Add or update data in a reference set.

Table 713. POST /reference\_data/sets/bulk\_load/{name} resource details

MIME Type
application/json

Table 714. POST /reference\_data/sets/bulk\_load/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 715. POST /reference\_data/sets/bulk\_load/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Array	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 716. POST /reference\_data/sets/bulk\_load/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

## Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables DEPRECATED

Retrieve a list of all reference tables.

Table 717. GET /reference\_data/tables resource details

MIME Type
application/json

Table 718. GET /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 719. GET /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "key_name_types": {
      "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    },
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## POST /reference\_data/tables DEPRECATED

Create a new reference table.

Table 720. POST /reference\_data/tables resource details

<b>MIME Type</b>
application/json

Table 721. POST /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create
element_type	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>key_name_types</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outer_key_label	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
key_name_types	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 722. POST /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid

Table 722. *POST /reference\_data/tables* response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables/{name} DEPRECATED

Return the reference table identified by name.

Return the reference table identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 723. *GET /reference\_data/tables/{name}* resource details

MIME Type
application/json

Table 724. *GET /reference\_data/tables/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 724. GET /reference\_data/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 725. GET /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "String": {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/tables/{name} DEPRECATED

Add or update an element in a reference table.

The value to be added must be of the appropriate type: either the type that corresponds to the innerKey predefined for the reference table, or the default elementType of the reference table

Table 726. POST /reference\_data/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 727. POST /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to add or update an element in
outer_key	query	Required	String	text/plain	Required - The outer key for the element to add or update
inner_key	query	Required	String	text/plain	Required - The inner key for the element to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 728. POST /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table



## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/tables/{name} DEPRECATED

Remove a reference table or purge its contents.

Table 729. DELETE /reference\_data/tables/{name} resource details

MIME Type
application/json

Table 730. DELETE /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 731. DELETE /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had its contents purged
204		The reference table has been removed
404	1002	The reference table does not exist
409	1004	The reference table could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

### Response Description

If the table was removed nothing is returned, otherwise information about the reference table that had its contents purged is returned.

### Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

### DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} DEPRECATED

Remove a value from a reference table.

Table 732. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} resource details

MIME Type
application/json

Table 733. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from
outer_key	path	Required	String	text/plain	Required - The outer key of the value to remove
inner_key	path	Required	String	text/plain	Required - The inner key of the value to remove

Table 733. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 734. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference table value

## Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /referencedata/mapOfSets DEPRECATED

Retrieve a list of all reference map of sets

Table 735. GET /referencedata/mapOfSets resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 736. GET /referencedata/mapOfSets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

### Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

### Response Sample

```
[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398377702319,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398377702319,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398377702319,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  }
]
```

## POST /referencedata/mapOfSets DEPRECATED

Create a new reference map of sets

Table 737. POST /referencedata/mapOfSets resource details

MIME Type
application/json

Table 738. POST /referencedata/mapOfSets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
keyLabel	query	Optional	String	text/plain	Optional - The label to describe the keys
valueLabel	query	Optional	String	text/plain	Optional - The label to describe the data values
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 739. POST /referencedata/mapOfSets response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid

Table 739. POST /referencedata/mapOfSets response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## GET /referencedata/mapOfSets/{name} DEPRECATED

Return the reference map of sets identified by **name**.

If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 740. GET /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 741. GET /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map of sets. The default value is 0.

Table 742. GET /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map of sets

## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 9,
  "data": {
    "String1": [
      {
        "value": "String",
        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
      },
      {
        "value": "String",
        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
      },
      {
        "value": "String",
        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
      }
    ],
    "String2": [
      {
        "value": "String",
        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
      },
      {
        "value": "String",
        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
      },
      {
        "value": "String",

```

```

        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
    }
],
"String3": [
{
"value": "String",
"source": "String",
"firstSeen": 1398377702319,
"lastSeen": 1398377702319
},
{
"value": "String",
"source": "String",
"firstSeen": 1398377702319,
"lastSeen": 1398377702319
},
{
"value": "String",
"source": "String",
"firstSeen": 1398377702319,
"lastSeen": 1398377702319
}
]
}
}

```

## POST /referencedata/mapOfSets/{name} DEPRECATED

Add or update an element in a reference map of sets

Table 743. POST /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 744. POST /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'



Table 745. *POST /referencedata/mapOfSets/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map of sets

## Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## DELETE /referencedata/mapOfSets/{name} DEPRECATED

Remove a map of sets or purge its contents

Table 746. *DELETE /referencedata/mapOfSets/{name}* resource details

MIME Type
application/json

Table 747. *DELETE /referencedata/mapOfSets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge

Table 747. DELETE /referencedata/mapOfSets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.

Table 748. DELETE /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map of sets does not exist
409	1004	The reference map of sets could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

## Response Description

If the reference map of sets was removed nothing is returned, otherwise information about the reference map of sets that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## DELETE /referencedata/mapOfSets/{name}/{key} DEPRECATED

Remove a value from a reference map of sets

Table 749. DELETE /referencedata/mapOfSets/{name}/{key} resource details

MIME Type
application/json

Table 750. DELETE /referencedata/mapOfSets/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 751. DELETE /referencedata/mapOfSets/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

### Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## GET /referencedata/maps DEPRECATED

Retrieve a list of all reference maps

Table 752. GET /referencedata/maps resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 753. GET /referencedata/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

### Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

### Response Sample

```
[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  }
]
```

## POST /referencedata/maps DEPRECATED

Create a new reference map

Table 754. POST /referencedata/maps resource details

MIME Type
application/json

Table 755. POST /referencedata/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create
keyLabel	query	Optional	String	text/plain	Optional - The label to describe the keys
valueLabel	query	Optional	String	text/plain	Optional - The label to describe the data values
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 756. POST /referencedata/maps response codes

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## GET /referencedata/maps/{name} DEPRECATED

Retrieve the reference map identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 757. GET /referencedata/maps/{name} resource details

MIME Type
application/json

Table 758. GET /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map. The default value is 0.

Table 759. GET /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1396355660000,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 3,
  "data": {
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    },
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    },
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    }
  }
}
```

## POST /referencedata/maps/{name} DEPRECATED

Add or update an element in a reference map

Table 760. POST /referencedata/maps/{name} resource details

MIME Type
application/json

Table 761. POST /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update

Table 761. POST /referencedata/maps/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 762. POST /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## DELETE /referencedata/maps/{name} DEPRECATED

Remove a reference map or purge its contents

Table 763. DELETE /referencedata/maps/{name} resource details

MIME Type
application/json



Table 764. DELETE /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.

Table 765. DELETE /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map does not exist
409	1004	The reference map could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

## Response Description

If the reference map was removed nothing is returned, otherwise information about the reference map that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## DELETE /referencedata/maps/{name}/{key} DEPRECATED

Remove a value from a reference map

Table 766. DELETE /referencedata/maps/{name}/{key} resource details

MIME Type
application/json

Table 767. DELETE /referencedata/maps/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 768. DELETE /referencedata/maps/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

### Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## GET /referencedata/sets DEPRECATED

Retrieve a list of all reference sets.

Table 769. GET /referencedata/sets resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 770. GET /referencedata/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

## Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

## Response Sample

```
[
  {
    "creationTime": 42,
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "numberOfElements": 42,
    "timeToLive": "String",
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## POST /referencedata/sets DEPRECATED

Create a new reference set

Table 771. POST /referencedata/sets resource details

<b>MIME Type</b>
application/json

Table 772. POST /referencedata/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created

Table 772. POST /referencedata/sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 773. POST /referencedata/sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398777706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 0
}
```

## GET /referencedata/sets/{name} DEPRECATED

Retrieve the reference set identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 774. GET /referencedata/sets/{name} resource details

<b>MIME Type</b>
application/json

Table 775. GET /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference set. The default value is 0.

Table 776. GET /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398277745579,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 3,
  "data": [
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398277745579,

```

```

    "lastSeen": 1398277745579
  },
  {
    "value": "String",
    "source": "String",
    "firstSeen": 1398277745579,
    "lastSeen": 1398277745579
  },
  {
    "value": "String",
    "source": "String",
    "firstSeen": 1398277745579,
    "lastSeen": 1398277745579
  }
]
}

```

## POST /referencedata/sets/{name} DEPRECATED

Add or update an element in a reference set

Table 777. POST /referencedata/sets/{name} resource details

MIME Type
application/json

Table 778. POST /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 779. POST /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update an element in the reference set

## Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 5
}
```

## DELETE /referencedata/sets/{name} DEPRECATED

Remove a reference set or purge its contents

Table 780. DELETE /referencedata/sets/{name} resource details

MIME Type
application/json

Table 781. DELETE /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.

Table 782. DELETE /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had its contents purged
204		The reference set has been removed
404	1002	The reference set does not exist
409	1004	The reference set could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference set

## Response Description

If the reference set was removed nothing is returned, otherwise information about the reference set that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398777706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 0
}
```

## DELETE /referencedata/sets/{name}/{value} DEPRECATED

Remove a value from a reference set

Table 783. DELETE /referencedata/sets/{name}/{value} resource details

<b>MIME Type</b>
application/json

Table 784. DELETE /referencedata/sets/{name}/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 785. DELETE /referencedata/sets/{name}/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had an value removed. This returns information about the reference set but not the contained data.



## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 5
}
```

## POST /referencedata/sets/bulkLoad/{name} DEPRECATED

Add or update data in a reference set

Table 786. POST /referencedata/sets/bulkLoad/{name} resource details

MIME Type
application/json

Table 787. POST /referencedata/sets/bulkLoad/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in

Table 788. POST /referencedata/sets/bulkLoad/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Object	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 789. POST /referencedata/sets/bulkLoad/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

## Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",

```

```

    "createdTime": 139877706999,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "numberOfElements": 0
}

```

## GET /referencedata/tables DEPRECATED

Retrieve a list of all reference tables

Table 790. GET /referencedata/tables resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 791. GET /referencedata/tables response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```

[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 139773789254,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
    "numberOfElements": 42,
    "keyNameTypes": {
      "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    }
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 139773789254,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
    "numberOfElements": 42,
    "keyNameTypes": {
      "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    }
  },
  {
    "name": "String",

```

```

"elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
"createdTime": 1397773789254,
"timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"numberOfElements": 42,
"keyNameTypes": {
  "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
}
}
]

```

## POST /referencedata/tables DEPRECATED

Create a new reference table

Table 792. POST /referencedata/tables resource details

<b>MIME Type</b>
application/json

Table 793. POST /referencedata/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create
elementType	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>keyNameTypes</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outerKeyLabel	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
keyNameTypes	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table

Table 794. POST /referencedata/tables response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created

Table 794. POST /referencedata/tables response codes (continued)

HTTP Response Code	Unique Code	Description
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 0,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```

## GET /referencedata/tables/{name} DEPRECATED

Return the reference table identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 795. GET /referencedata/tables/{name} resource details

MIME Type
application/json

Table 796. GET /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.

Table 796. GET /referencedata/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference table. The default value is 0.

Table 797. GET /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "ALN",
  "createdTime": 1398888888888,
  "timeoutType": "LAST_SEEN",
  "timeToLive": "0 years 1 mons 0 days 0 hours 0 mins 0.00 secs",
  "key1Label": "String",
  "numberOfElements": 6,
  "keyNameTypes": {
    "String1": "ALN",
    "String2": "ALN",
    "String3": "ALN"
  },
  "data": {
    "String2": {
      "String1": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      }
    },
    "String3": {
      "String1": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      }
    },
    "String2": {
```



Table 799. POST /referencedata/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 800. POST /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table

## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 5,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```

## DELETE /referencedata/tables/{name} DEPRECATED

Remove a reference table or purge its contents

Table 801. DELETE /referencedata/tables/{name} resource details

MIME Type
application/json

Table 802. DELETE /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge

Table 802. DELETE /referencedata/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.

Table 803. DELETE /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had its contents purged
204		The reference table has been removed
404	1002	The reference table does not exist
409	1004	The reference table could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

## Response Description

If the table was removed nothing is returned, otherwise information about the reference table that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 0,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```



## DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} DEPRECATED

Remove a value from a reference table

Table 804. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} resource details

MIME Type
application/json

Table 805. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from
outerKey	path	Required	String	text/plain	Required - The outer key of the value to remove
innerKey	path	Required	String	text/plain	Required - The inner key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 806. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference table value

### Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
}
```

```

"key1Label": "String",
"numberOfElements": 5,
"keyNameTypes": {
  "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
}
}

```

## Scanner endpoints

Use the references for REST API V4 scanner endpoints.

### GET /scanner/profiles DEPRECATED

Retrieves all of the currently created scan profiles. No parameters are required and the following information should be retrieved for each scan profile - scanProfileId - scanProfileName - description - scanType - scannerName

Table 807. GET /scanner/profiles resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 808. GET /scanner/profiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

### Response Description

The list of scan profiles currently configured in QVM

### Response Sample

### POST /scanner/profiles/create DEPRECATED

Initiates a request to create a new scanProfile. The request takes one parameter - createScanRequest, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and ips to scan e.g. {'name':'New Scan Profile', 'ips':['10.100.85.135']}

Table 809. POST /scanner/profiles/create resource details

<b>MIME Type</b>
text/plain

Table 810. POST /scanner/profiles/create request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 811. POST /scanner/profiles/create response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
419	9101	Occurs when a parameter is missing or invalid
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

### Response Description

An indicator of whether the scan has been created successfully or not.

### Response Sample

String

### POST /scanner/profiles/start DEPRECATED

Initiates a request to start an already created scanProfile.

The request takes one parameter - scanProfileId. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The scanProfileId will be validated and an appropriate message returned.

Table 812. POST /scanner/profiles/start resource details

MIME Type
text/plain

Table 813. POST /scanner/profiles/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
scanProfileId	query	Required	String	text/plain	The unique id of the scan profile we want to start

Table 814. POST /scanner/profiles/start response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

### Response Description

An indicator of whether the scan has been started successfully or not.

### Response Sample

String

## GET /scanner/scanprofiles DEPRECATED

Retrieves all of the currently created scan profiles. No parameters are required and the following information should be retrieved for each scan profile - scanProfileId - name - description - scanType - scannerName - schedule - status - progress - endTime - duration

Table 815. GET /scanner/scanprofiles resource details

<b>MIME Type</b>
application/json

Table 816. GET /scanner/scanprofiles request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 817. GET /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

### Response Description

The list of scan profiles currently configured in QVM

### Response Sample

```
[
  {
    "description": "String",
```

```

    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
  }
]

```

## POST /scanner/scanprofiles DEPRECATED

Initiates a request to create a new scanProfile.

The request takes one parameter - createScanRequest, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and hosts to scan e.g. {'name':'New Scan Profile', 'hosts':['10.100.85.135']}

Table 818. POST /scanner/scanprofiles resource details

MIME Type
text/plain

Table 819. POST /scanner/scanprofiles request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	Object	application/json	null	{ "description": "String", "hosts": [ "String" ], "name": "String" }

Table 820. POST /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been created successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles/{profileid} DEPRECATED

Retrieves a scan profile for a given Scan Profile ID. The only parameter required is the Scan Profile ID. The following information about a scan profile will be returned - scanProfileId - name - description - scanType - scannerName - schedule - status - progress - endTime - duration

Table 821. GET /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 822. GET /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we need to retrieve information for
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 823. GET /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
200		The scan profile was successfully returned

Table 823. GET /scanner/scanprofiles/{profileid} response codes (continued)

HTTP Response Code	Unique Code	Description
500	1030	Occurs when an attempt is made to list a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
  }
]
```

## POST /scanner/scanprofiles/{profileid} DEPRECATED

Update a scan profile.

The Scan Profile ID is required. The following information on a scan profile can be updated - name - description - ips e.g. {'name':'Updated Scan Profile', 'ips':['10.100.85.135']}

Table 824. POST /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 825. *POST /scanner/scanprofiles/{profileid}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile used to update

Table 826. *POST /scanner/scanprofiles/{profileid}* request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 827. *POST /scanner/scanprofiles/{profileid}* response codes

HTTP Response Code	Unique Code	Description
202		The scan profile was successfully updated
500	1030	Occurs when an attempt is made to update a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

A message to indicate whether the scan profile has updated or not.

## Response Sample

### **DELETE /scanner/scanprofiles/{profileid} DEPRECATED**

Initiates a request to delete a scanProfile. The request takes one parameter - the Scan Profile ID.

Table 828. *DELETE /scanner/scanprofiles/{profileid}* resource details

MIME Type
text/plain

Table 829. *DELETE /scanner/scanprofiles/{profileid}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	null

Table 830. *DELETE /scanner/scanprofiles/{profileid}* response codes

HTTP Response Code	Unique Code	Description
204		The scan has been successfully deleted
500	1030	Occurs when an attempt is made to delete a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been deleted successfully or not.



## Response Sample

String

## POST /scanner/scanprofiles/{profileid}/start DEPRECATED

Initiates a request to start an already created scanProfile.

The request takes one parameter - scanProfileId, and one optional parameter - ips. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The scanProfileId will be validated and an appropriate message returned.

Table 831. POST /scanner/scanprofiles/{profileid}/start resource details

MIME Type
text/plain

Table 832. POST /scanner/scanprofiles/{profileid}/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we want to start

Table 833. POST /scanner/scanprofiles/{profileid}/start request body details

Parameter	Data Type	MIME Type	Description	Sample
ips	JSON	application/json	null	null

Table 834. POST /scanner/scanprofiles/{profileid}/start response codes

HTTP Response Code	Unique Code	Description
202		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## SIEM endpoints

Use the references for REST API V3.1 SIEM endpoints.

## GET /siem/local\_destination\_addresses DEPRECATED

Retrieve a list of local destination addresses currently in the system.

Table 835. GET /siem/local\_destination\_addresses resource details

<b>MIME Type</b>
application/json

Table 836. GET /siem/local\_destination\_addresses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list based on the contents of various fields.

Table 837. GET /siem/local\_destination\_addresses response codes

HTTP Response Code	Unique Code	Description
200		The local destination address list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the local destination address list was being retrieved.

### Response Description

An array of local destination address objects. A local destination address object contains the following fields:

- **id** - Number - The ID of the destination address.
- **local\_destination\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the destination address.
- **network** - String - The network of the destination address.

- **offense\_ids** - Array of Numbers - List of offense IDs the destination address is part of.
- **source\_address\_ids** - Array of Numbers - List of source address IDs associated with the destination address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the destination address.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

### Response Sample

```
[
  {
    "domain_id": 42,
    "event_flow_count": 42,
    "first_event_flow_seen": 42,
    "id": 42,
    "last_event_flow_seen": 42,
    "local_destination_ip": "String",
    "magnitude": 42,
    "network": "String",
    "offense_ids": [
      42
    ],
    "source_address_ids": [
      42
    ]
  }
]
```

### GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} DEPRECATED

Retrieve an offense local destination address.

Table 838. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} resource details

MIME Type
application/json

Table 839. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
local_destination_address_id	path	Required	Number (Integer)	text/plain	Required - The ID of the local destination address to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 840. GET /siem/local\_destination\_addresses/{local\_destination\_address\_id} response codes

HTTP Response Code	Unique Code	Description
200		The local destination was retrieved.
404	1002	No local destination address was found for the provided local_destination_address_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the local destination address was being retrieved.

## Response Description

A local destination address object. A local destination address object contains the following fields:

- **id** - Number - The ID of the destination address.
- **local\_destination\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the destination address.
- **network** - String - The network of the destination address.
- **offense\_ids** - Array of Numbers - List of offense IDs the destination address is part of.
- **source\_address\_ids** - Array of Numbers - List of source address IDs associated with the destination address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the destination address.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
{
  "domain_id": 42,
  "event_flow_count": 42,
  "first_event_flow_seen": 42,
  "id": 42,
  "last_event_flow_seen": 42,
  "local_destination_ip": "String",
  "magnitude": 42,
  "network": "String",
  "offense_ids": [
    42
  ],
  "source_address_ids": [
    42
  ]
}
```

## GET /siem/offense\_closing\_reasons DEPRECATED

Retrieve a list of all offense closing reasons.

Table 841. GET /siem/offense\_closing\_reasons resource details

<b>MIME Type</b>
application/json

Table 842. GET /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
include_reserved	query	Optional	Boolean	text/plain	Optional - If true, reserved closing reasons are included in the response. Defaults to false. Reserved closing reasons cannot be used to close an offense.
include_deleted	query	Optional	Boolean	text/plain	Optional - If true, deleted closing reasons are included in the response. Defaults to false. Deleted closing reasons cannot be used to close an offense.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 843. GET /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
200		The closing reasons list was retrieved.
500	1020	An error occurred while the closing reasons list was being retrieved.

### Response Description

An array of ClosingReason objects. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

### Response Sample

```
[
  {
    "id": 42,
    "is_deleted": true,
    "is_reserved": true,
    "text": "String"
  }
]
```

### POST /siem/offense\_closing\_reasons DEPRECATED

Create an offense closing reason.

Table 844. POST /siem/offense\_closing\_reasons resource details

MIME Type
application/json

Table 845. POST /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
reason	query	Required	String	text/plain	Required - The text of the offense closing reason must be 5 - 60 characters in length.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 846. POST /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
201		The closing reason was created.
409	1004	The closing reason already exists.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create the closing reason.

## Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

## Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

## GET /siem/offense\_closing\_reasons/{closing\_reason\_id} DEPRECATED

Retrieve an offense closing reason.

Table 847. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} resource details

MIME Type
application/json

Table 848. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
closing_reason_id	path	Required	Number (Integer)	text/plain	Required - The closing reason ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 849. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} response codes

HTTP Response Code	Unique Code	Description
200		The closing reason was retrieved.
404	1002	No closing reason was found for the provided closing_reason_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the closing reason.

## Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

## Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

## GET /siem/offenses DEPRECATED

Retrieve a list of offenses currently in the system.

Table 850. GET /siem/offenses resource details

MIME Type
application/json

Table 851. GET /siem/offenses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.



Table 852. GET /siem/offenses response codes

HTTP Response Code	Unique Code	Description
200		The offense list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the offense list was being retrieved.

## Response Description

An array of Offense objects. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense. Filtering is not supported on this field.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense. Filtering is not supported on this field.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.

- **offense\_source** - String - The source of the offense. Filtering is not supported on this field.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED". The following operators are not supported when you filter on this field: "<", ">", "<=", ">=", "BETWEEN".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers - The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 853. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
[{"credibility": 42,
  "source_address_ids": [42],
  "remote_destination_count": 42,
  "local_destination_address_ids": [42]
}, {"assigned_to": "String",
  "local_destination_count": 42,
  "source_count": 42,
  "start_time": 42,
  "id": 42,
  "destination_networks": ["String"],
  "inactive": true,
  "protected": true,
  "policy_category_count": 42,
  "description": "String",
  "category_count": 42,
  "domain_id": 42,
  "relevance": 42,
  "device_count": 42,
  "security_category_count": 42,
  "flow_count": 42,
  "event_count": 42,
  "offense_source": "String",
  "status": "String <one of: OPEN, HIDDEN, CLOSED>",
  "magnitude": 42,
  "severity": 42,
  "username_count": 42,
  "closing_user": "String",
  "follow_up": true,
  "closing_reason_id": 42,
  "close_time": 42,
  "source_network": "String",
  "last_updated_time": 42,
  "categories": ["String"],
  "offense_type": 42}]
```

## GET /siem/offenses/{offense\_id} DEPRECATED

Retrieve an offense structure that describes properties of an offense

Table 854. GET /siem/offenses/{offense\_id} resource details

<b>MIME Type</b>
application/json

Table 855. GET /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 856. GET /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense was being retrieved.

## Response Description

An Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.

- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers - The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.
- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 857. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

### Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
```

```

"close_time": 42,
"closing_reason_id": 42,
"closing_user": "String",
"credibility": 42,
"description": "String",
"destination_networks": [
  "String"
],
"device_count": 42,
"domain_id": 42,
"event_count": 42,
"flow_count": 42,
"follow_up": true,
"id": 42,
"inactive": true,
"last_updated_time": 42,
"local_destination_address_ids": [
  42
],
"local_destination_count": 42,
"magnitude": 42,
"offense_source": "String",
"offense_type": 42,
"policy_category_count": 42,
"protected": true,
"relevance": 42,
"remote_destination_count": 42,
"security_category_count": 42,
"severity": 42,
"source_address_ids": [
  42
],
"source_count": 42,
"source_network": "String",
"start_time": 42,
"status": "String <one of: OPEN, HIDDEN, CLOSED>",
"username_count": 42
}

```

## POST /siem/offenses/{offense\_id} DEPRECATED

Update an offense.

Table 858. POST /siem/offenses/{offense\_id} resource details

MIME Type
application/json

Table 859. POST /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The ID of the offense to update.
protected	query	Optional	Boolean	text/plain	Optional - Set to true to protect the offense.
follow_up	query	Optional	Boolean	text/plain	Optional - Set to true to set the follow up flag on the offense.

Table 859. POST /siem/offenses/{offense\_id} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
status	query	Optional	String	text/plain	Optional - The new status for the offense. Set to one of: OPEN, HIDDEN, CLOSED. When the status of an offense is being set to CLOSED, a valid closing_reason_id must be provided. To hide an offense, use the HIDDEN status. To show a previously hidden offense, use the OPEN status.
closing_reason_id	query	Optional	Number (Integer)	text/plain	Optional - The ID of a closing reason. You must provide a valid closing_reason_id when you close an offense.
assigned_to	query	Optional	String	text/plain	Optional - A user to assign the offense to.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 860. POST /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was updated.
403	1009	User does not have the required capability to assign an offense.
404	1002	No offense was found for the provided offense_id.
409	1008	Request cannot be completed due to the state of the offense.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense was being updated.

## Response Description

An updated Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.

- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.
- **source\_address\_ids** - Array of numbers - The source address IDs that are associated with the offense.
- **local\_destination\_address\_ids** - Array of numbers - The local destination address IDs that are associated with the offense.



- **domain\_id** - Number - Optional. ID of associated domain if the offense is associated with a single domain.

Table 861. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
  "close_time": 42,
  "closing_reason_id": 42,
  "closing_user": "String",
  "credibility": 42,
  "description": "String",
  "destination_networks": [
    "String"
  ],
  "device_count": 42,
  "domain_id": 42,
  "event_count": 42,
  "flow_count": 42,
  "follow_up": true,
  "id": 42,
  "inactive": true,
  "last_updated_time": 42,
  "local_destination_address_ids": [
    42
  ],
  "local_destination_count": 42,
  "magnitude": 42,
  "offense_source": "String",
  "offense_type": 42,
  "policy_category_count": 42,
}
```

```

    "protected": true,
    "relevance": 42,
    "remote_destination_count": 42,
    "security_category_count": 42,
    "severity": 42,
    "source_address_ids": [
      42
    ],
    "source_count": 42,
    "source_network": "String",
    "start_time": 42,
    "status": "String <one of: OPEN, HIDDEN, CLOSED>",
    "username_count": 42
  }

```

## GET /siem/offenses/{offense\_id}/notes DEPRECATED

Retrieve a list of notes for an offense.

Table 862. GET /siem/offenses/{offense\_id}/notes resource details

<b>MIME Type</b>
application/json

Table 863. GET /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the notes for.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 864. GET /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
200		The note list was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the note list was being retrieved.

## Response Description

An array of Note objects. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
[
  {
    "create_time": 42,
    "id": 42,
    "note_text": "String",
    "username": "String"
  }
]
```

## POST /siem/offenses/{offense\_id}/notes DEPRECATED

Create a note on an offense.

Table 865. POST /siem/offenses/{offense\_id}/notes resource details

MIME Type
application/json

Table 866. POST /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to add the note to.
note_text	query	Required	String	text/plain	Required - The note text.

Table 866. POST /siem/offenses/{offense\_id}/notes request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 867. POST /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
201		The note was created.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create the note.

## Response Description

The Note object that was created. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## GET /siem/offenses/{offense\_id}/notes/{note\_id} DEPRECATED

Retrieve a note for an offense.

Table 868. GET /siem/offenses/{offense\_id}/notes/{note\_id} resource details

MIME Type
application/json

Table 869. GET /siem/offenses/{offense\_id}/notes/{note\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the note from.
note_id	path	Required	Number (Integer)	text/plain	Required - The note ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 870. GET /siem/offenses/{offense\_id}/notes/{note\_id} response codes

HTTP Response Code	Unique Code	Description
200		The note was retrieved.
404	1002	No offense was found for the provided offense_id.
404	1003	No note was found for the provided note_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the note.

## Response Description

The Note object for the note ID. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## GET /siem/source\_addresses DEPRECATED

Retrieve a list offense source addresses currently in the system.

Table 871. GET /siem/source\_addresses resource details

<b>MIME Type</b>
application/json

Table 872. GET /siem/source\_addresses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 873. GET /siem/source\_addresses response codes

HTTP Response Code	Unique Code	Description
200		The source address list was retrieved.
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the source address list was being retrieved.

### Response Description

An array of source address objects. A source address object contains the following fields:

- **id** - Number - The ID of the source.
- **source\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the source address.
- **network** - String - The network of the source address.

- **offense\_ids** - Array of Numbers - List of offense IDs the source is part of.
- **local\_destination\_address\_ids** - Array of Numbers - List of local destination address IDs associated with the source address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the source.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

### Response Sample

```
[
  {
    "domain_id": 42,
    "event_flow_count": 42,
    "first_event_flow_seen": 42,
    "id": 42,
    "last_event_flow_seen": 42,
    "local_destination_address_ids": [
      42
    ],
    "magnitude": 42,
    "network": "String",
    "offense_ids": [
      42
    ],
    "source_ip": "String"
  }
]
```

### GET /siem/source\_addresses/{source\_address\_id} DEPRECATED

Retrieve an offense source address.

Table 874. GET /siem/source\_addresses/{source\_address\_id} resource details

MIME Type
application/json

Table 875. GET /siem/source\_addresses/{source\_address\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
source_address_id	path	Required	Number (Integer)	text/plain	Required - The ID of the source address to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 876. GET /siem/source\_addresses/{source\_address\_id} response codes

HTTP Response Code	Unique Code	Description
200		The source address was retrieved.
404	1002	No source address was found for the provided source_address_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the source address was being retrieved.

## Response Description

A source address object. A source address object contains the following fields:

- **id** - Number - The ID of the source.
- **source\_ip** - String - The IP address.
- **magnitude** - Number - The magnitude of the source address.
- **network** - String - The network of the source address.
- **offense\_ids** - Array of Numbers - List of offense IDs the source is part of.
- **local\_destination\_address\_ids** - Array of Numbers - List of local destination address IDs associated with the source address.
- **event\_flow\_count** - Number - The number of events and flows that are associated with the source.
- **first\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the first event or flow was seen.
- **last\_event\_flow\_seen** - Number - The number of milliseconds since epoch when the last event or flow was seen.
- **domain\_id** - Number - The ID of associated domain.

## Response Sample

```
{
  "domain_id": 42,
  "event_flow_count": 42,
  "first_event_flow_seen": 42,
  "id": 42,
  "last_event_flow_seen": 42,
  "local_destination_address_ids": [
    42
  ],
  "magnitude": 42,
  "network": "String",
  "offense_ids": [
    42
  ],
  "source_ip": "String"
}
```

---

## REST API V3.0 References

Each API reference provides information about the parameters, mime type, stability, and responses for each endpoint.

### Ariel endpoints

Use the references for REST API V3.0 ariel endpoints.



## GET /ariel/databases DEPRECATED

Retrieve Ariel database names

Retrieve a list of available Ariel databases.

Table 877. GET /ariel/databases resource details

<b>MIME Type</b>
application/json

Table 878. GET /ariel/databases request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 879. GET /ariel/databases response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of Ariel databases.

### Response Description

The names of the available Ariel databases.

### Response Sample

```
[  
  "String"  
]
```

## GET /ariel/databases/{database\_name} DEPRECATED

Retrieve the columns defined for a specific Ariel database.

Retrieve the columns that are defined for the specified Ariel database. This is the set of columns that can be explicitly named in the column list of a SELECT query.

Table 880. GET /ariel/databases/{database\_name} resource details

<b>MIME Type</b>
application/json

Table 881. GET /ariel/databases/{database\_name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
database_name	path	Required	String	text/plain	Required. The name of the Ariel database that contains the columns that you want to retrieve.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 882. GET /ariel/databases/{database\_name} response codes

HTTP Response Code	Unique Code	Description
200		The database columns were retrieved.
404	1002	The database does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the database columns.

## Response Description

A list of columns that are defined for the specified database. Multiple properties of each column are returned. For example, the column name or an indication that the column is indexable.

## Response Sample

```
{
  "columns": [
    {
      "argument_type": "String",
      "indexable": true,
      "name": "String"
    }
  ]
}
```

## GET /ariel/searches DEPRECATED

Retrieve Ariel search\_ids.

Retrieve the list of Ariel searches. This includes search\_ids for completed and active searches.

Table 883. GET /ariel/searches resource details

MIME Type
application/json

Table 884. GET /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 885. GET /ariel/searches response codes

HTTP Response Code	Unique Code	Description
200		The search list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of searches.

### Response Description

A list of search IDs.

### Response Sample

```
[  
  "String"  
]
```

## POST /ariel/searches DEPRECATED

Create a new asynchronous Ariel search

Create an Ariel search based on Ariel Query Language (AQL) query expressions. A search\_id is returned with the search results. Searches are executed asynchronously. In subsequent API calls, you can use this search\_id to determine the status of the search and retrieve the results.

This endpoint only accepts SELECT and RUN query expressions.

Queries are applied to the range of data in a time interval. The default time interval is the last 60 seconds. You can specify an alternate time interval in your query expression. For more information, see the AQL Reference Guide.

Table 886. POST /ariel/searches resource details

<b>MIME Type</b>
application/json

Table 887. POST /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
query_expression	query	Required	String	text/plain	Required. The AQL query to execute.
search_id	query	Optional	String	text/plain	Optional. A custom search_id value for the new search to replace the system generated search_id. The search_id must be unique and is only used for SELECT query expressions. The search_id can only contain numbers, letters, dashes, and underscores.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 888. POST /ariel/searches response codes

HTTP Response Code	Unique Code	Description
201		An Ariel search was successfully created.
409	1004	The search could not be created. The search_id provided is already in use. Use a unique search_id.
422	2000	The query_expression contains invalid AQL syntax.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create a new search.

## Response Description

Information about the specified search, including the search\_id. Use the search\_id to access or manipulate the search with the other API endpoints.

If the search has the same search criteria as an existing search, the response message returns a reference to the original search\_id and does not create a new search.

### Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

### GET /ariel/searches/{search\_id} DEPRECATED

Retrieve information about an Ariel search

Retrieve status information for a search, based on the search\_id parameter. The same informational fields are returned regardless of whether the search is in progress or is complete.

Table 889. GET /ariel/searches/{search\_id} resource details

<b>MIME Type</b>
application/json

Table 890. GET /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The identifier for an Ariel search.

Table 890. GET /ariel/searches/{search\_id} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 891. GET /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search information was retrieved.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search information.

## Response Description

Information about the specified search, including the search status.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## POST /ariel/searches/{search\_id} DEPRECATED

Update an Ariel search.

Update details for an Ariel search. You can update searches in the following ways:

- To cancel an active search, set the **status** parameter to CANCELED. This stops the search and keeps any search results that were collected before the search was canceled.
- The results for a completed search can be saved by setting the **save\_results** parameter to true. This ensures that the search is not automatically removed when it expires in accordance with the retention policy.

The Ariel server uses an internal retention policy to manage available disk space. Searches might be deleted automatically, according to the settings of the retention policy. Searches with saved results are not automatically reclaimed by the server and are therefore retained. A search can be explicitly deleted by using the DELETE /searches/{search\_id} endpoint.

Note: Saving too many search results might result in insufficient disk space to process new searches.

Table 892. POST /ariel/searches/{search\_id} resource details

<b>MIME Type</b>
application/json

Table 893. POST /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The ID of the search to update.
save_results	query	Optional	String	text/plain	Optional. The only accepted value is true. If this value is provided, the search results will not be deleted by the search expiration removal process.
status	query	Optional	String	text/plain	Optional. The only accepted value is CANCELED. If this value is provided, the search will be canceled.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 894. POST /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search was updated.
404	1002	The search does not exist.
409	1008	The current status of the search prevented the search results from being saved.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to update the search.

## Response Description

Information about the specified search that was updated.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## DELETE /ariel/searches/{search\_id} DEPRECATED

Delete an Ariel search.

Deletes an Ariel search. This discards collected results and stops the search if it in progress. This search is deleted regardless of whether the results were saved.

Table 895. DELETE /ariel/searches/{search\_id} resource details

MIME Type
application/json



Table 896. DELETE /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The search_id of the search to delete.

Table 897. DELETE /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
204		The search was deleted.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to delete the search.

## Response Description

There is no response body for a successfully deleted Ariel Search.

## Response Sample

```
{
  "error_messages": [
    {
      "code": "String <one of: ERROR_FILE_ACCESS,
        ERROR_CURSOR_CREATE,
        ERROR_CURSOR_CREATE_EXISTS,
        WARN_MAX_RECORDS,
        WARN_MAX_COLLECTED_RECORDS,
        ERROR_INVALID_CURSOR,
        ERROR_PROTECT_CURSOR,
        ERROR_SERVER_IO,
        WARN_INTERRUPT,
        ERROR_READ_TIMEOUT,
        ERROR_INVALID_QUERY_PARAMS,
        WARN_QUERY_TIME_LIMIT,
        ERROR_GENERAL_FAILURE,
        ERROR_FILE_RUNTIME_EXCEPTION,
        ERROR_INVALID_QUERY,
        WARN_CANCEL,
        INFO_INVALID_SORTING,
        ERROR_FETCH,
        WARN_SHARING_VIOLATION,
        WARN_INCOMPLETE_RESULT,
        ERROR_QUERY_EXPIRED,
        INFO_MAINTENANCE,
        ERROR_FUNCTION_ERROR,
        ERROR_COULD_NOT_CONNECT,
        ERROR_RB_COMMUNICATION,
        ERROR_RB_SOURCE_DATABLOCK_SEND,
        ERROR_RB_DESTINATION_DATABLOCK_RECEIVE,
        NEXUS_ERROR>",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ]
}
```

## GET /ariel/searches/{search\_id}/results DEPRECATED

Retrieves search results in the requested format.

Retrieve the results of the Ariel search that is identified by the search\_id. The Accepts request header indicates the format of the result. The format can be JSON, CSV, XML, or tabular text.

By default, all query result records are returned. To restrict the results to a contiguous subset of the records, you can supply a Range header to specify the inclusive range of records to be returned.

This end-point works with query results that are generated by AQL query expressions. This endpoint might not work as expected for results that are generated by other means. Search results might not be retrievable for searches that are created on the Console.

The response samples are for the following query: Select sourceIP, destinationIP from events.

Table 898. GET /ariel/searches/{search\_id}/results resource details

MIME Type
application/json application/csv text/table application/xml

Table 899. GET /ariel/searches/{search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	The ID of the search criteria for the returned results.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 900. GET /ariel/searches/{search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The search results were retrieved.
404	1002	The search does not exist.
404	1003	Search results not found. The search is still in progress.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search results.

## Response Description

The search results for the specified search\_id. The format that is used to encapsulate the data depends on the format specified in the Accept header for this request.

## Response Sample

```
{
  "events": [
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    },
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    }
  ]
}
```

## Asset model endpoints

Use the references for REST API V4 Asset Model endpoints.

### GET /asset\_model/assets DEPRECATED

List all assets found in the model.

List all assets found in the model.

Table 901. GET /asset\_model/assets resource details

MIME Type
application/json

Table 902. GET /asset\_model/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 902. GET /asset\_model/assets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 903. GET /asset\_model/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
500	1020	The server encountered an error while trying to retrieve the assets.

## Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[{"id": 42, "interfaces": [{"first_seen_scanner": 42,
                          "id": 42,
                          "first_seen_profiler": 42,
                          "created": 42,
                          "last_seen_profiler": 42,
                          "last_seen_scanner": 42,
                          "mac_address": "String",
                          "ip_addresses": [{"first_seen_scanner": 42,
                                             "id": 42,
                                             "first_seen_profiler": 42,
                                             "created": 42,
                                             "network_id": 42,
                                             "value": "String",
                                             "last_seen_profiler": 42,
                                             "last_seen_scanner": 42,
                                             "type": "String"}]}],
  "properties": [{"id": 42,
                  "name": "String",
                  "value": "String",
                  "last_reported": 42,
                  "type_id": 42,
                  "last_reported_by": "String"}]}]
```

## POST /asset\_model/assets/{asset\_id} DEPRECATED

Update an asset with several pertinent pieces of information.

Update an asset with several pertinent pieces of information. The **asset\_id** tag is mandatory, and is the unique identifier for an asset. This field is available through the **/asset\_model/assets** or **/asset\_model/saved\_searches/{saved\_search\_id}/results** query. To update properties, the property type id which is available through the **/asset\_model/properties** query should be provided along with the new value. See the sample provided demonstrating an example asset update.

Table 904. *POST /asset\_model/assets/{asset\_id}* resource details

<b>MIME Type</b>
text/plain

Table 905. *POST /asset\_model/assets/{asset\_id}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
asset_id	path	Required	String	text/plain	Unique identifier of the asset to update.

Table 906. *POST /asset\_model/assets/{asset\_id}* request body details

Parameter	Data Type	MIME Type	Description	Sample
asset	JSON	application/json	JSON representation of an asset.	{ "properties": [ { "type_id": 1001, "value": "given name value" }, { "type_id": 1002, "value": "unified name value" } ] }

Table 907. *POST /asset\_model/assets/{asset\_id}* response codes

HTTP Response Code	Unique Code	Description
202		The request to update the asset was successful. The update will take place when the asset profile application receives the request.
422	1005	One or more of the requested property updates were invalid.
500	1020	The server encountered an error registering the update with the asset profile application.

## Response Description

Information about the asset that was updated.

## Response Sample

String

## GET /asset\_model/properties DEPRECATED

Get a list of available asset property types that can be used.

Get a list of available asset property types that can be used or applied against the */asset\_model/assets* endpoint.

Table 908. *GET /asset\_model/properties* resource details

<b>MIME Type</b>
application/json

Table 909. GET /asset\_model/properties request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 910. GET /asset\_model/properties response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of asset property types completed successfully.
500	1020	An error occurred while trying to retrieve the list of asset property types.

## Response Description

List of asset properties. Per asset property type: id and name that make up this asset property type.

## Response Sample

```
[
  {
    "custom": true,
    "data_type": "String",
    "display": true,
    "id": 42,
    "name": "String",
    "state": 42
  }
]
```

## GET /asset\_model/saved\_searches DEPRECATED

Get a list of saved searches that can be used.

Get a list of saved searches that can be used or applied against the `/asset_model/saved_searches/{saved_search_id}/results` query.

Table 911. GET /asset\_model/saved\_searches resource details

<b>MIME Type</b>
application/json

Table 912. GET /asset\_model/saved\_searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 913. GET /asset\_model/saved\_searches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully.
500	1020	The server encountered an error while trying to retrieve the list of saved searches.

## Response Description

List of saved searches. Per saved search: id, name and list of filters that make up this saved search

## Response Sample

```
[
  {
    "columns": [
      {
        "name": "String",
```

```

        "type": "String"
    }
  ],
  "description": "String",
  "filters": [
    {
      "operator": "String",
      "parameter": "String",
      "value": "String"
    }
  ],
  "id": 42,
  "name": "String"
}
]

```

## GET /asset\_model/saved\_searches/{saved\_search\_id}/results DEPRECATED

Retrieves a list of assets based on the results of an asset saved search.

Retrieves a list of assets based on the results of an asset saved search.

Table 914. GET /asset\_model/saved\_searches/{saved\_search\_id}/results resource details

MIME Type
application/json

Table 915. GET /asset\_model/saved\_searches/{saved\_search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
saved_search_id	path	Required	String	text/plain	Unique identifier of the saved search used to retrieve assets.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.



Table 916. GET /asset\_model/saved\_searches/{saved\_search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
422	1005	The unique identifier of the saved search provided was invalid.
500	1003	The server encountered an error executing the saved search.

## Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[
  {
    "id": 42,
    "interfaces": [
      {
        "created": 42,
        "first_seen_profiler": 42,
        "first_seen_scanner": 42,
        "id": 42,
        "ip_addresses": [
          {
            "created": 42,
            "first_seen_profiler": 42,
            "first_seen_scanner": 42,
            "id": 42,
            "last_seen_profiler": 42,
            "last_seen_scanner": 42,
            "network_id": 42,
            "type": "String",
            "value": "String"
          }
        ],
        "last_seen_profiler": 42,
        "last_seen_scanner": 42,
        "mac_address": "String"
      }
    ],
    "properties": [
      {
        "id": 42,
        "last_reported": 42,
        "last_reported_by": "String",
        "name": "String",
        "type_id": 42,
        "value": "String"
      }
    ]
  }
]
```

## Authentication endpoints

Use the references for REST API V3.0 authentication endpoints.

## POST /auth/logout DEPRECATED

Invoke this method as an authorized user and your session will be invalidated.

Table 917. POST /auth/logout resource details

<b>MIME Type</b>
text/plain

There are no parameters for this endpoint.

Table 918. POST /auth/logout response codes

HTTP Response Code	Unique Code	Description
200		The session was invalidated.

### Response Description

Returns true. Throws exception upon failure.

### Response Sample

true

## Help endpoints

Use the references for REST API V3.0 help endpoints.

## GET /help/capabilities DEPRECATED

List all QRadar API capabilities

List the QRadar API capabilities. The response will contain all available RESTful resources We allow every authenticated user to access this method, but restrict the output based on their user capabilities

Table 919. GET /help/capabilities resource details

<b>MIME Type</b>
application/json

Table 920. GET /help/capabilities request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
categories	query	Optional	Array<String>	application/json	Optional - Restrict your search to this list of capabilities
paths	query	Optional	Array<String>	application/json	Optional - Restrict your search to these paths only
httpMethods	query	Optional	Array<String>	application/json	Optional - Restrict your search to these HTTP methods
version	query	Optional	String	text/plain	Optional - Restrict your search to this version (or below)
showExperimental	query	Optional	Boolean	text/plain	Optional - If true, we include experimental endpoints (default is true)
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 920. GET /help/capabilities request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 921. GET /help/capabilities response codes

HTTP Response Code	Unique Code	Description
200		The API capabilities list was retrieved.
422	1001	Invalid input
422	1002	Our internal mapping has an unexpected structure or contains an invalid element value
500	1003	A generic error has occurred while retrieving our capabilities

## Response Description

Endpoints you are able to access, mapped against versions they belong to. If full content is not requested, values will be null.

## Response Sample

```
{
  "categories": [
    {
      "apis": [
        {
          "httpMethod": "String <one of: OPTIONS,
            GET,
            HEAD,
            POST,
            PUT,
            DELETE,
            TRACE,
            CONNECT,
            PATCH>",
          "operations": [
            {
              "additionalFiltering": true,
              "deprecated": true,
              "description": "String",
              "errorResponses": [
                {
                  "code": 42,
                  "description": "String",
                  "uniqueCode": 42
                }
              ],
              "httpMethod": "String",
              "lastSupportedVersion": "String",
              "parameters": [
                {
                  "allowMultiple": true,
                  "defaultValue": "String",
                  "description": "String",

```

```

        "name": "String",
        "pathIndex": 42,
        "required": true,
        "source": "String",
        "supportedContentTypes": [
            {
                "dataType": "String",
                "mimeType": "String",
                "sample": "String"
            }
        ]
    },
    "removalTarget": "String",
    "removed": true,
    "responseClass": "String",
    "responseDescription": {
        "description": "String",
        "properties": [
            {
                "description": "String",
                "name": "String"
            }
        ]
    },
    "successResponses": [
        {
            "code": 42,
            "description": "String"
        }
    ],
    "summary": "String",
    "supportedContentTypes": [
        {
            "dataType": "String",
            "mimeType": "String",
            "sample": "String"
        }
    ],
    "version": "String",
    "visibility": "String"
    },
    "path": "String"
    },
    "path": "String"
    },
    "path": "String"
}

```

## QRadar Vulnerability Manager endpoints

Use the references for REST API V4 QRadar Vulnerability Manager endpoints.

### GET /qvm/assets DEPRECATED

List the assets with discovered vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 922. GET /qvm/assets resource details

<b>MIME Type</b>
application/json

Table 923. GET /qvm/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 924. GET /qvm/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by asset completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of assets data

## Response Sample

### GET /qvm/filters DEPRECATED

Get a list of the allowable filters that can be used or applied against /qvm endpoints.

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 925. GET /qvm/filters resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 926. GET /qvm/filters response codes

HTTP Response Code	Unique Code	Description
200		The search executed successfully
420	9102	An error occurred while executing the search

## Response Description

list of Filters.

## Response Sample

### GET /qvm/network DEPRECATED

List the networks present in the asset model with vulnerabilities present. The response will contain all available RESTful resources

Table 927. GET /qvm/network resource details

<b>MIME Type</b>
application/json

Table 928. GET /qvm/network request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 929. GET /qvm/network response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by network completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of network related data

## Response Sample

### GET /qvm/openservices DEPRECATED

List the openservices present in the asset model with vulnerabilities present. The response will contain all available RESTful resources

Table 930. GET /qvm/openservices resource details

<b>MIME Type</b>
application/json

Table 931. GET /qvm/openservices request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name

Table 931. GET /qvm/openservices request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 932. GET /qvm/openservices response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by open service completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of open services related data

## Response Sample

### GET /qvm/savedsearches DEPRECATED

Get a list of saved searches that can be applied against /qvm endpoints.

A list of saved searches that can be applied against the following endpoints:

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 933. GET /qvm/savedsearches resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 934. GET /qvm/savedsearches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully
420	9103	An error occurred while trying to retrieve the list of saved searches

## Response Description

list of saved searches. Per saved search: id, name and list of filters that make up this saved search

## Response Sample

### POST /qvm/tickets/assign DEPRECATED

Update the remediation ticket for the assigned vulnerability

Table 935. POST /qvm/tickets/assign resource details

<b>MIME Type</b>
application/json

Table 936. POST /qvm/tickets/assign request body details

Parameter	Data Type	MIME Type	Description	Sample
ticket	JSON	application/json	<p>'ticketId': required.</p> <p>'priority' one of required : Critical, Major, Minor, Warning, Informational.</p> <p>'status' one of required : Opened, Fixed, Re-Opened, Closed .</p> <p>'dueDate' Optional : yyyy-MM-dd HH:mm:ss.</p> <p>'assignedUser' required : valid QRadar user account name or a valid email.</p> <p>'comment' Optional : text.</p> <p>'commentUser' Optional : valid QRadar user account name, if not included will default current API user.</p>	[ { "ticketId":"1000", "status":"Opened", "priority":"Critical", "dueDate":"2015-01-04 12:00:00", "assignedUser":"admin", "comment":"testComment", "commentUser":"admin" } ]

Table 937. POST /qvm/tickets/assign response codes

HTTP Response Code	Unique Code	Description
200		The request to assign a ticket completed successfully
420	9104	An error occurred while trying to assign a ticket due to invalid arguments

## Response Description

success message if update succeed



## Response Sample

### GET /qvm/vulninstances DEPRECATED

List the Vulnerability Instances present in the asset model. The response will contain all available RESTful resources

Table 938. GET /qvm/vulninstances resource details

<b>MIME Type</b>
application/json

Table 939. GET /qvm/vulninstances request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 940. GET /qvm/vulninstances response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by instance completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability instance data

## Response Sample

### GET /qvm/vulns DEPRECATED

List the Vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 941. GET /qvm/vulns resource details

<b>MIME Type</b>
application/json

Table 942. GET /qvm/vulns request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name

Table 942. GET /qvm/vulns request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 943. GET /qvm/vulns response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability data

## Response Sample

## Reference Data endpoints

Use the references for REST API V3 Reference Data endpoints.

### GET /reference\_data/map\_of\_sets DEPRECATED

Retrieve a list of all reference map of sets.

Retrieve a list of all reference map of sets.

Table 944. GET /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 945. GET /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 945. GET /reference\_data/map\_of\_sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 946. GET /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

## Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## POST /reference\_data/map\_of\_sets DEPRECATED

Create a new reference map of sets.

Create a new reference map of sets.

Table 947. POST /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 948. POST /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 949. POST /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.

Table 949. *POST /reference\_data/map\_of\_sets* response codes (continued)

HTTP Response Code	Unique Code	Description
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/map\_of\_sets/{name} DEPRECATED

Return the reference map of sets identified by name.

Return the reference map of sets identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 950. *GET /reference\_data/map\_of\_sets/{name}* resource details

MIME Type
application/json

Table 951. *GET /reference\_data/map\_of\_sets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 951. GET /reference\_data/map\_of\_sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 952. GET /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map of sets

## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": [
      {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    ]
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/map\_of\_sets/{name} DEPRECATED

Add or update an element in a reference map of sets.

Add or update an element in a reference map of sets.

Table 953. POST /reference\_data/map\_of\_sets/{name} resource details

<b>MIME Type</b>
application/json

Table 954. POST /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 955. POST /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map of sets

## Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name} DEPRECATED

Remove a map of sets or purge its contents.

Remove a map of sets or purge its contents.

Table 956. DELETE /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 957. DELETE /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.



Table 957. DELETE /reference\_data/map\_of\_sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 958. DELETE /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map of sets does not exist
409	1004	The reference map of sets could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

## Response Description

If the reference map of sets was removed nothing is returned, otherwise information about the reference map of sets that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name}/{key} DEPRECATED

Remove a value from a reference map of sets.

Remove a value from a reference map of sets.

Table 959. DELETE /reference\_data/map\_of\_sets/{name}/{key} resource details

<b>MIME Type</b>
application/json

Table 960. DELETE /reference\_data/map\_of\_sets/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 961. DELETE /reference\_data/map\_of\_sets/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

## Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps DEPRECATED

Retrieve a list of all reference maps.

Retrieve a list of all reference maps.

Table 962. GET /reference\_data/maps resource details

MIME Type
application/json

Table 963. GET /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 964. GET /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

## Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## POST /reference\_data/maps DEPRECATED

Create a new reference map.

Create a new reference map.

Table 965. POST /reference\_data/maps resource details

MIME Type
application/json

Table 966. POST /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 966. POST /reference\_data/maps request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 967. POST /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps/{name} DEPRECATED

Retrieve the reference map identified by name.

Retrieve the reference map identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 968. GET /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 969. GET /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 970. GET /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/maps/{name} DEPRECATED

Add or update an element in a reference map.

Add or update an element in a reference map.

Table 971. POST /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 972. POST /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 972. *POST /reference\_data/maps/{name}* request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 973. *POST /reference\_data/maps/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/maps/{name} DEPRECATED

Remove a reference map or purge its contents.

Remove a reference map or purge its contents.



Table 974. DELETE /reference\_data/maps/{name} resource details

<b>MIME Type</b>
application/json

Table 975. DELETE /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 976. DELETE /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map does not exist
409	1004	The reference map could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

## Response Description

If the reference map was removed nothing is returned, otherwise information about the reference map that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/maps/{name}/{key} DEPRECATED

Remove a value from a reference map.

Remove a value from a reference map.

Table 977. DELETE /reference\_data/maps/{name}/{key} resource details

MIME Type
application/json

Table 978. DELETE /reference\_data/maps/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 979. DELETE /reference\_data/maps/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map

Table 979. DELETE /reference\_data/maps/{name}/{key} response codes (continued)

HTTP Response Code	Unique Code	Description
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

## Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/sets DEPRECATED

Retrieve a list of all reference sets.

Retrieve a list of all reference sets.

Table 980. GET /reference\_data/sets resource details

MIME Type
application/json

Table 981. GET /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 981. GET /reference\_data/sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 982. GET /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

## Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## POST /reference\_data/sets DEPRECATED

Create a new reference set.

Create a new reference set.

Table 983. POST /reference\_data/sets resource details

MIME Type
application/json

Table 984. POST /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created

Table 984. *POST /reference\_data/sets request parameter details (continued)*

Parameter	Type	Optionality	Data Type	MIME Type	Description
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 985. *POST /reference\_data/sets response codes*

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/sets/{name} DEPRECATED

Retrieve the reference set identified by name.

Retrieve the reference set identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 986. GET /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 987. GET /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 988. GET /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": [
    {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  ],
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/{name} DEPRECATED

Add or update an element in a reference set.

Add or update an element in a reference set.

Table 989. POST /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 990. POST /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 990. POST /reference\_data/sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 991. POST /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update an element in the reference set

## Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/sets/{name} DEPRECATED

Remove a reference set or purge its contents.

Remove a reference set or purge its contents.

Table 992. DELETE /reference\_data/sets/{name} resource details

MIME Type
application/json



Table 993. DELETE /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 994. DELETE /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had its contents purged
204		The reference set has been removed
404	1002	The reference set does not exist
409	1004	The reference set could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference set

## Response Description

If the reference set was removed nothing is returned, otherwise information about the reference set that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
```

```

    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## DELETE /reference\_data/sets/{name}/{value} DEPRECATED

Remove a value from a reference set.

Remove a value from a reference set.

Table 995. DELETE /reference\_data/sets/{name}/{value} resource details

MIME Type
application/json

Table 996. DELETE /reference\_data/sets/{name}/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 997. DELETE /reference\_data/sets/{name}/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had a value removed. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/bulk\_load/{name} DEPRECATED

Add or update data in a reference set.

Add or update data in a reference set.

Table 998. POST /reference\_data/sets/bulk\_load/{name} resource details

MIME Type
application/json

Table 999. POST /reference\_data/sets/bulk\_load/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1000. POST /reference\_data/sets/bulk\_load/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Array	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 1001. POST /reference\_data/sets/bulk\_load/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated

Table 1001. POST /reference\_data/sets/bulk\_load/{name} response codes (continued)

HTTP Response Code	Unique Code	Description
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

## Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables DEPRECATED

Retrieve a list of all reference tables.

Retrieve a list of all reference tables.

Table 1002. GET /reference\_data/tables resource details

MIME Type
application/json

Table 1003. GET /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1003. GET /reference\_data/tables request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1004. GET /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "key_name_types": {
      "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    },
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## GET /reference\_data/tables/{name} DEPRECATED

Return the reference table identified by name.

Return the reference table identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1005. GET /reference\_data/tables/{name} resource details

MIME Type
application/json

Table 1006. GET /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 1007. GET /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "String": {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
}
```

```

    "key_name_types": {
      "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    },
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
}

```

## POST /reference\_data/tables/{name} DEPRECATED

Add or update an element in a reference table.

Add or update an element in a reference table. The value to be added must be of the appropriate type: either the type that corresponds to the innerKey predefined for the reference table, or the default elementType of the reference table

Table 1008. POST /reference\_data/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 1009. POST /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to add or update an element in
outer_key	query	Required	String	text/plain	Required - The outer key for the element to add or update
inner_key	query	Required	String	text/plain	Required - The inner key for the element to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 1009. POST /reference\_data/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1010. POST /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table

## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/tables/{name} DEPRECATED

Remove a reference table or purge its contents.

Remove a reference table or purge its contents.

Table 1011. DELETE /reference\_data/tables/{name} resource details

MIME Type
application/json



Table 1012. DELETE /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1013. DELETE /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had its contents purged
204		The reference table has been removed
404	1002	The reference table does not exist
409	1004	The reference table could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

## Response Description

If the table was removed nothing is returned, otherwise information about the reference table that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
```

```

    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} DEPRECATED

Remove a value from a reference table.

Remove a value from a reference table.

Table 1014. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} resource details

MIME Type
application/json

Table 1015. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from
outer_key	path	Required	String	text/plain	Required - The outer key of the value to remove
inner_key	path	Required	String	text/plain	Required - The inner key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1016. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed

Table 1016. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference table value

## Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/tables DEPRECATED

Create a new reference table.

Create a new reference table.

Table 1017. POST /reference\_data/tables resource details

MIME Type
application/json

Table 1018. POST /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create

Table 1018. POST /reference\_data/tables request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
element_type	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>key_name_types</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outer_key_label	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
key_name_types	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1019. POST /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /referencedata/mapOfSets DEPRECATED

Retrieve a list of all reference map of sets

Table 1020. GET /referencedata/mapOfSets resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 1021. GET /referencedata/mapOfSets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

## Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

## Response Sample

```
[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398377702319,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398377702319,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",

```

```

"elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
"createdTime": 1398377702319,
"timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"valueLabel": "String",
"numberOfElements": 42
}
]

```

## POST /referencedata/mapOfSets DEPRECATED

Create a new reference map of sets

Table 1022. POST /referencedata/mapOfSets resource details

<b>MIME Type</b>
application/json

Table 1023. POST /referencedata/mapOfSets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
keyLabel	query	Optional	String	text/plain	Optional - The label to describe the keys
valueLabel	query	Optional	String	text/plain	Optional - The label to describe the data values
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 1024. POST /referencedata/mapOfSets response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## GET /referencedata/mapOfSets/{name} DEPRECATED

Return the reference map of sets identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1025. GET /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 1026. GET /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map of sets. The default value is 0.

Table 1027. GET /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map of sets

## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139837702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 9,
  "data": {
    "String1": [
      {
        "value": "String",
        "source": "String",
        "firstSeen": 139837702319,
        "lastSeen": 139837702319
      },
      {
        "value": "String",
        "source": "String",
        "firstSeen": 139837702319,
        "lastSeen": 139837702319
      },
      {
        "value": "String",
        "source": "String",
        "firstSeen": 139837702319,
        "lastSeen": 139837702319
      }
    ],
    "String2": [
      {
        "value": "String",
        "source": "String",
        "firstSeen": 139837702319,
        "lastSeen": 139837702319
      },
      {
        "value": "String",
        "source": "String",
        "firstSeen": 139837702319,
        "lastSeen": 139837702319
      }
    ]
  }
}
```



```

    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    }
  ],
  "String3": [
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    },
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    },
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    }
  ]
}

```

## POST /referencedata/mapOfSets/{name} DEPRECATED

Add or update an element in a reference map of sets

Table 1028. POST /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 1029. POST /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1029. POST /referencedata/mapOfSets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'

Table 1030. POST /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map of sets

## Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## DELETE /referencedata/mapOfSets/{name} DEPRECATED

Remove a map of sets or purge its contents

Table 1031. DELETE /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 1032. DELETE /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge

Table 1032. DELETE /referencedata/mapOfSets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.

Table 1033. DELETE /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map of sets does not exist
409	1004	The reference map of sets could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

## Response Description

If the reference map of sets was removed nothing is returned, otherwise information about the reference map of sets that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## DELETE /referencedata/mapOfSets/{name}/{key} DEPRECATED

Remove a value from a reference map of sets

Table 1034. DELETE /referencedata/mapOfSets/{name}/{key} resource details

MIME Type
application/json

Table 1035. DELETE /referencedata/mapOfSets/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1036. DELETE /referencedata/mapOfSets/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

### Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## GET /referencedata/maps DEPRECATED

Retrieve a list of all reference maps

Table 1037. GET /referencedata/maps resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 1038. GET /referencedata/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

### Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

### Response Sample

```
[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  }
]
```

## POST /referencedata/maps DEPRECATED

Create a new reference map

Table 1039. POST /referencedata/maps resource details

MIME Type
application/json

Table 1040. POST /referencedata/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create
keyLabel	query	Optional	String	text/plain	Optional - The label to describe the keys
valueLabel	query	Optional	String	text/plain	Optional - The label to describe the data values
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 1041. POST /referencedata/maps response codes

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## GET /referencedata/maps/{name} DEPRECATED

Retrieve the reference map identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1042. GET /referencedata/maps/{name} resource details

<b>MIME Type</b>
application/json

Table 1043. GET /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map. The default value is 0.

Table 1044. GET /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1396355660000,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 3,
  "data": {
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    },
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    },
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    }
  }
}
```

## POST /referencedata/maps/{name} DEPRECATED

Add or update an element in a reference map

Table 1045. POST /referencedata/maps/{name} resource details

MIME Type
application/json

Table 1046. POST /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update



Table 1046. POST /referencedata/maps/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 1047. POST /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## DELETE /referencedata/maps/{name} DEPRECATED

Remove a reference map or purge its contents

Table 1048. DELETE /referencedata/maps/{name} resource details

MIME Type
application/json

Table 1049. DELETE /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.

Table 1050. DELETE /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map does not exist
409	1004	The reference map could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

## Response Description

If the reference map was removed nothing is returned, otherwise information about the reference map that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## DELETE /referencedata/maps/{name}/{key} DEPRECATED

Remove a value from a reference map

Table 1051. DELETE /referencedata/maps/{name}/{key} resource details

MIME Type
application/json

Table 1052. DELETE /referencedata/maps/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1053. DELETE /referencedata/maps/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

### Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## GET /referencedata/sets DEPRECATED

Retrieve a list of all reference sets.

Table 1054. GET /referencedata/sets resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 1055. GET /referencedata/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

## Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

## Response Sample

```
[
  {
    "creationTime": 42,
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "numberOfElements": 42,
    "timeToLive": "String",
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## POST /referencedata/sets DEPRECATED

Create a new reference set

Table 1056. POST /referencedata/sets resource details

<b>MIME Type</b>
application/json

Table 1057. POST /referencedata/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created

Table 1057. POST /referencedata/sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 1058. POST /referencedata/sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398777706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 0
}
```

## GET /referencedata/sets/{name} DEPRECATED

Retrieve the reference set identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1059. GET /referencedata/sets/{name} resource details

<b>MIME Type</b>
application/json

Table 1060. GET /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference set. The default value is 0.

Table 1061. GET /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398277745579,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 3,
  "data": [
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398277745579,
```

```

    "lastSeen": 1398277745579
  },
  {
    "value": "String",
    "source": "String",
    "firstSeen": 1398277745579,
    "lastSeen": 1398277745579
  },
  {
    "value": "String",
    "source": "String",
    "firstSeen": 1398277745579,
    "lastSeen": 1398277745579
  }
]
}

```

## POST /referencedata/sets/{name} DEPRECATED

Add or update an element in a reference set

Table 1062. POST /referencedata/sets/{name} resource details

MIME Type
application/json

Table 1063. POST /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 1064. POST /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update an element in the reference set

## Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 5
}
```

## DELETE /referencedata/sets/{name} DEPRECATED

Remove a reference set or purge its contents

Table 1065. DELETE /referencedata/sets/{name} resource details

MIME Type
application/json

Table 1066. DELETE /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.

Table 1067. DELETE /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had its contents purged
204		The reference set has been removed
404	1002	The reference set does not exist
409	1004	The reference set could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference set



## Response Description

If the reference set was removed nothing is returned, otherwise information about the reference set that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398777706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 0
}
```

## DELETE /referencedata/sets/{name}/{value} DEPRECATED

Remove a value from a reference set

Table 1068. DELETE /referencedata/sets/{name}/{value} resource details

<b>MIME Type</b>
application/json

Table 1069. DELETE /referencedata/sets/{name}/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1070. DELETE /referencedata/sets/{name}/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had an value removed. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 5
}
```

## POST /referencedata/sets/bulkLoad/{name} DEPRECATED

Add or update data in a reference set

Table 1071. POST /referencedata/sets/bulkLoad/{name} resource details

MIME Type
application/json

Table 1072. POST /referencedata/sets/bulkLoad/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in

Table 1073. POST /referencedata/sets/bulkLoad/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Object	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 1074. POST /referencedata/sets/bulkLoad/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

## Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",

```

```

    "createdTime": 139877706999,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "numberOfElements": 0
}

```

## GET /referencedata/tables DEPRECATED

Retrieve a list of all reference tables

Table 1075. GET /referencedata/tables resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 1076. GET /referencedata/tables response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```

[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1397773789254,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
    "numberOfElements": 42,
    "keyNameTypes": {
      "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    }
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1397773789254,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
    "numberOfElements": 42,
    "keyNameTypes": {
      "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
      "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    }
  },
  {
    "name": "String",

```

```

"elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
"createdTime": 1397773789254,
"timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"numberOfElements": 42,
"keyNameTypes": {
  "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
}
}
]

```

## POST /referencedata/tables DEPRECATED

Create a new reference table

Table 1077. POST /referencedata/tables resource details

<b>MIME Type</b>
application/json

Table 1078. POST /referencedata/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create
elementType	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>keyNameTypes</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outerKeyLabel	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
keyNameTypes	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table

Table 1079. POST /referencedata/tables response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created

Table 1079. POST /referencedata/tables response codes (continued)

HTTP Response Code	Unique Code	Description
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 0,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```

## GET /referencedata/tables/{name} DEPRECATED

Return the reference table identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1080. GET /referencedata/tables/{name} resource details

MIME Type
application/json

Table 1081. GET /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.

Table 1081. GET /referencedata/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference table. The default value is 0.

Table 1082. GET /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "ALN",
  "createdTime": 1398888888888,
  "timeoutType": "LAST_SEEN",
  "timeToLive": "0 years 1 mons 0 days 0 hours 0 mins 0.00 secs",
  "key1Label": "String",
  "numberOfElements": 6,
  "keyNameTypes": {
    "String1": "ALN",
    "String2": "ALN",
    "String3": "ALN"
  },
  "data": {
    "String2": {
      "String1": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      }
    },
    "String3": {
      "String1": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      }
    },
    "String2": {
```

```

        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
    },
    "String1": {
        "String1": {
            "value": "String",
            "source": "String",
            "firstSeen": 1398888888888,
            "lastSeen": 1398888888888
        },
        "String2": {
            "value": "String",
            "source": "String",
            "firstSeen": 1398888888888,
            "lastSeen": 1398888888888
        },
        "String3": {
            "value": "String",
            "source": "String",
            "firstSeen": 1398888888888,
            "lastSeen": 1398888888888
        }
    }
}
}
}
}
}

```

### POST /referencedata/tables/{name} DEPRECATED

Add or update an element in a reference table. The value to be added must be of the appropriate type: either the type that corresponds to the innerKey predefined for the reference table, or the default elementType of the reference table

Table 1083. POST /referencedata/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 1084. POST /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to add or update an element in
outerKey	query	Required	String	text/plain	Required - The outer key for the element to add or update
innerKey	query	Required	String	text/plain	Required - The inner key for the element to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1084. POST /referencedata/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 1085. POST /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table

## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 5,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```

## DELETE /referencedata/tables/{name} DEPRECATED

Remove a reference table or purge its contents

Table 1086. DELETE /referencedata/tables/{name} resource details

MIME Type
application/json

Table 1087. DELETE /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge



Table 1087. DELETE /referencedata/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.

Table 1088. DELETE /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had its contents purged
204		The reference table has been removed
404	1002	The reference table does not exist
409	1004	The reference table could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

## Response Description

If the table was removed nothing is returned, otherwise information about the reference table that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 0,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```

## DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} DEPRECATED

Remove a value from a reference table

Table 1089. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} resource details

MIME Type
application/json

Table 1090. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from
outerKey	path	Required	String	text/plain	Required - The outer key of the value to remove
innerKey	path	Required	String	text/plain	Required - The inner key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1091. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference table value

### Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
```

```

"key1Label": "String",
"numberOfElements": 5,
"keyNameTypes": {
  "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
}
}

```

## Scanner endpoints

Use the references for REST API V4 scanner endpoints.

### GET /scanner/profiles DEPRECATED

Retrieves all of the currently created scan profiles. No parameters are required and the following information should be retrieved for each scan profile - scanProfileId - scanProfileName - description - scanType - scannerName

Table 1092. GET /scanner/profiles resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 1093. GET /scanner/profiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

### Response Description

The list of scan profiles currently configured in QVM

### Response Sample

### POST /scanner/scanprofiles DEPRECATED

Initiates a request to create a new scanProfile. The request takes one parameter - createScanRequest, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and hosts to scan e.g. {'name':'New Scan Profile', 'hosts':['10.100.85.135']}

Table 1094. POST /scanner/scanprofiles resource details

<b>MIME Type</b>
text/plain

Table 1095. POST /scanner/scanprofiles request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	Object	application/json	null	{ "description": "String", "hosts": [ "String" ], "name": "String" }

Table 1096. POST /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

### Response Description

An indicator of whether the scan has been created successfully or not.

### Response Sample

String

### POST /scanner/profiles/create DEPRECATED

Initiates a request to create a new scanProfile. The request takes one parameter - createScanRequest, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and ips to scan e.g. `{'name':'New Scan Profile', 'ips':['10.100.85.135']}`

Table 1097. POST /scanner/profiles/create resource details

MIME Type
text/plain

Table 1098. POST /scanner/profiles/create request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 1099. POST /scanner/profiles/create response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
419	9101	Occurs when a parameter is missing or invalid
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

### Response Description

An indicator of whether the scan has been created successfully or not.

### Response Sample

String

### POST /scanner/profiles/start DEPRECATED

Initiates a request to start an already created scanProfile. The request takes one parameter - scanProfileId. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The scanProfileId will be validated and an appropriate message returned.

Table 1100. POST /scanner/profiles/start resource details

<b>MIME Type</b>
text/plain

Table 1101. POST /scanner/profiles/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
scanProfileId	query	Required	String	text/plain	The unique id of the scan profile we want to start

Table 1102. POST /scanner/profiles/start response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles DEPRECATED

Retrieves all of the currently created scan profiles. No parameters are required and the following information should be retrieved for each scan profile - scanProfileId - name - description - scanType - scannerName - schedule - status - progress - endTime - duration

Table 1103. GET /scanner/scanprofiles resource details

<b>MIME Type</b>
application/json

Table 1104. GET /scanner/scanprofiles request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1104. GET /scanner/scanprofiles request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 1105. GET /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
  }
]
```

```

        "scannerName": "String",
        "schedule": "String",
        "status": "String"
    }
]

```

### GET /scanner/scanprofiles/{profileid} DEPRECATED

Retrieves a scan profile for a given Scan Profile ID. The only parameter required is the Scan Profile ID. The following information about a scan profile will be returned - scanProfileId - name - description - scanType - scannerName - schedule - status - progress - endTime - duration

Table 1106. GET /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 1107. GET /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we need to retrieve information for
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 1108. GET /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
200		The scan profile was successfully returned
500	1030	Occurs when an attempt is made to list a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
  }
]
```

## POST /scanner/scanprofiles/{profileid} DEPRECATED

Update a scan profile. The Scan Profile ID is required. The following information on a scan profile can be updated - name - description - ips eg {'name': 'Updated Scan Profile', 'ips': ['10.100.85.135']}

Table 1109. POST /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 1110. POST /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile used to update

Table 1111. POST /scanner/scanprofiles/{profileid} request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null



Table 1112. *POST /scanner/scanprofiles/{profileid}* response codes

HTTP Response Code	Unique Code	Description
202		The scan profile was successfully updated
500	1030	Occurs when an attempt is made to update a scan profile when certain conditions are not met, or when too many scan requests have been made

### Response Description

A message to indicate whether the scan profile has updated or not.

### Response Sample

#### **DELETE /scanner/scanprofiles/{profileid} DEPRECATED**

Initiates a request to delete a scanProfile. The request takes one parameter - the Scan Profile ID.

Table 1113. *DELETE /scanner/scanprofiles/{profileid}* resource details

MIME Type
text/plain

Table 1114. *DELETE /scanner/scanprofiles/{profileid}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	null

Table 1115. *DELETE /scanner/scanprofiles/{profileid}* response codes

HTTP Response Code	Unique Code	Description
204		The scan has been successfully deleted
500	1030	Occurs when an attempt is made to delete a scan when certain conditions are not met, or when too many scan requests have been made

### Response Description

An indicator of whether the scan has been deleted successfully or not.

### Response Sample

String

#### **POST /scanner/scanprofiles/{profileid}/start DEPRECATED**

Initiates a request to start an already created scanProfile. The request takes one parameter - scanProfileId, and one optional parameter - ips. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The scanProfileId will be validated and an appropriate message returned.

Table 1116. POST /scanner/scanprofiles/{profileid}/start resource details

<b>MIME Type</b>
text/plain

Table 1117. POST /scanner/scanprofiles/{profileid}/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we want to start

Table 1118. POST /scanner/scanprofiles/{profileid}/start request body details

Parameter	Data Type	MIME Type	Description	Sample
ips	JSON	application/json	null	null

Table 1119. POST /scanner/scanprofiles/{profileid}/start response codes

HTTP Response Code	Unique Code	Description
202		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## SIEM endpoints

Use the references for REST API V3 SIEM endpoints.

### GET /siem/offense\_closing\_reasons DEPRECATED

Retrieve a list of all offense closing reasons.

Table 1120. GET /siem/offense\_closing\_reasons resource details

<b>MIME Type</b>
application/json

Table 1121. GET /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
include_reserved	query	Optional	Boolean	text/plain	Optional - If true, reserved closing reasons are included in the response. Defaults to false. Reserved closing reasons cannot be used to close an offense.
include_deleted	query	Optional	Boolean	text/plain	Optional - If true, deleted closing reasons are included in the response. Defaults to false. Deleted closing reasons cannot be used to close an offense.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1122. GET /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
200		The closing reasons list was retrieved.
500	1020	An error occurred while the closing reasons list was being retrieved.

## Response Description

An array of ClosingReason objects. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.
- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.

- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

### Response Sample

```
[
  {
    "id": 42,
    "is_deleted": true,
    "is_reserved": true,
    "text": "String"
  }
]
```

## POST /siem/offense\_closing\_reasons DEPRECATED

Create an offense closing reason.

Table 1123. POST /siem/offense\_closing\_reasons resource details

MIME Type
application/json

Table 1124. POST /siem/offense\_closing\_reasons request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
reason	query	Required	String	text/plain	Required - The text of the offense closing reason must be 5 - 60 characters in length.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1125. POST /siem/offense\_closing\_reasons response codes

HTTP Response Code	Unique Code	Description
201		The closing reason was created.
409	1004	The closing reason already exists.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create the closing reason.

### Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.

- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

### Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

### GET /siem/offense\_closing\_reasons/{closing\_reason\_id} DEPRECATED

Retrieve an offense closing reason.

Table 1126. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} resource details

MIME Type
application/json

Table 1127. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
closing_reason_id	path	Required	Number (Integer)	text/plain	Required - The closing reason ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1128. GET /siem/offense\_closing\_reasons/{closing\_reason\_id} response codes

HTTP Response Code	Unique Code	Description
200		The closing reason was retrieved.
404	1002	No closing reason was found for the provided closing_reason_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the closing reason.

### Response Description

A ClosingReason object. A closing reason object contains the following fields:

- **id** - Number - The ID of the closing reason.
- **text** - String - The text of the closing reason.

- **is\_deleted** - Boolean - Determines whether the closing reason is deleted. Deleted closing reasons cannot be used to close an offense.
- **is\_reserved** - Boolean - Determines whether the closing reason is reserved. Reserved closing reasons cannot be used to close an offense.

### Response Sample

```
{
  "id": 42,
  "is_deleted": true,
  "is_reserved": true,
  "text": "String"
}
```

### GET /siem/offenses DEPRECATED

Retrieve a list of offenses currently in the system.

Retrieve a list of offenses currently in the system.

Table 1129. GET /siem/offenses resource details

MIME Type
application/json

Table 1130. GET /siem/offenses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1131. GET /siem/offenses response codes

HTTP Response Code	Unique Code	Description
200		The offense list was retrieved.

Table 1131. GET /siem/offenses response codes (continued)

HTTP Response Code	Unique Code	Description
422	1005	A request parameter is not valid.
422	1010	The filter parameter is not valid.
500	1020	An error occurred while the offense list was being retrieved.

## Response Description

An array of Offense objects. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense. Filtering is not supported on this field.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense. Filtering is not supported on this field.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.

- **offense\_source** - String - The source of the offense. Filtering is not supported on this field.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED". The following operators are not supported when you filter on this field: "<", ">", "<=", ">=", "BETWEEN".
- **username\_count** - The number of usernames that are associated with the offense.

Table 1132. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

### Response Sample

```
[{"credibility": 42,
  "remote_destination_count": 42,
  "assigned_to": "String",
  "local_destination_count": 42,
  "source_count": 42,
  "start_time": 42,
  "id": 42,
  "destination_networks": ["String"],
  "inactive": true,
  "protected": true,
```



```

"policy_category_count": 42,
"description": "String",
"category_count": 42,
"relevance": 42,
"device_count": 42,
"security_category_count": 42,
"flow_count": 42,
"event_count": 42,
"offense_source": "String",
"status": "String <one of: OPEN,
          HIDDEN,
          CLOSED>",

"magnitude": 42,
"severity": 42,
"username_count": 42,
"closing_user": "String",
"follow_up": true,
"closing_reason_id": 42,
"close_time": 42,
"source_network": "String",
"last_updated_time": 42,
"categories": ["String"],
"offense_type": 42}]

```

## GET /siem/offenses/{offense\_id} DEPRECATED

Retrieve an offense structure that describes properties of an offense

Retrieve an offense structure that describes properties of an offense

Table 1133. GET /siem/offenses/{offense\_id} resource details

MIME Type
application/json

Table 1134. GET /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1135. GET /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.

Table 1135. GET /siem/offenses/{offense\_id} response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while the offense was being retrieved.

## Response Description

An Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.

- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.

Table 1136. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
  "close_time": 42,
  "closing_reason_id": 42,
  "closing_user": "String",
  "credibility": 42,
  "description": "String",
  "destination_networks": [
    "String"
  ],
  "device_count": 42,
  "event_count": 42,
  "flow_count": 42,
  "follow_up": true,
  "id": 42,
```

```

    "inactive": true,
    "last_updated_time": 42,
    "local_destination_count": 42,
    "magnitude": 42,
    "offense_source": "String",
    "offense_type": 42,
    "policy_category_count": 42,
    "protected": true,
    "relevance": 42,
    "remote_destination_count": 42,
    "security_category_count": 42,
    "severity": 42,
    "source_count": 42,
    "source_network": "String",
    "start_time": 42,
    "status": "String <one of: OPEN, HIDDEN, CLOSED>",
    "username_count": 42
  }

```

## POST /siem/offenses/{offense\_id} DEPRECATED

Update an offense.

Table 1137. POST /siem/offenses/{offense\_id} resource details

MIME Type
application/json

Table 1138. POST /siem/offenses/{offense\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The ID of the offense to update.
protected	query	Optional	Boolean	text/plain	Optional - Set to true to protect the offense.
follow_up	query	Optional	Boolean	text/plain	Optional - Set to true to set the follow up flag on the offense.
status	query	Optional	String	text/plain	Optional - The new status for the offense. Set to one of: OPEN, HIDDEN, CLOSED. When the status of an offense is being set to CLOSED, a valid closing_reason_id must be provided. To hide an offense, use the HIDDEN status. To show a previously hidden offense, use the OPEN status.
closing_reason_id	query	Optional	Number (Integer)	text/plain	Optional - The ID of a closing reason. You must provide a valid closing_reason_id when you close an offense.
assigned_to	query	Optional	String	text/plain	Optional - A user to assign the offense to.

Table 1138. POST /siem/offenses/{offense\_id} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1139. POST /siem/offenses/{offense\_id} response codes

HTTP Response Code	Unique Code	Description
200		The offense was updated.
403	1009	User does not have the required capability to assign an offense.
404	1002	No offense was found for the provided offense_id.
409	1008	Request cannot be completed due to the state of the offense.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense was being updated.

## Response Description

An updated Offense object. An Offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **closing\_user** - String - The user that closed the offense.
- **closing\_reason\_id** - Number - The ID of the offense closing reason. The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.

- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.
- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **follow\_up** - Boolean - True if the offense is marked for follow up.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.

Table 1140. Offense Type Codes

Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule

Table 1140. Offense Type Codes (continued)

Code	Offense Type
15	App Id
18	Scheduled Search

### Response Sample

```
{
  "assigned_to": "String",
  "categories": [
    "String"
  ],
  "category_count": 42,
  "close_time": 42,
  "closing_reason_id": 42,
  "closing_user": "String",
  "credibility": 42,
  "description": "String",
  "destination_networks": [
    "String"
  ],
  "device_count": 42,
  "event_count": 42,
  "flow_count": 42,
  "follow_up": true,
  "id": 42,
  "inactive": true,
  "last_updated_time": 42,
  "local_destination_count": 42,
  "magnitude": 42,
  "offense_source": "String",
  "offense_type": 42,
  "policy_category_count": 42,
  "protected": true,
  "relevance": 42,
  "remote_destination_count": 42,
  "security_category_count": 42,
  "severity": 42,
  "source_count": 42,
  "source_network": "String",
  "start_time": 42,
  "status": "String <one of: OPEN, HIDDEN, CLOSED>",
  "username_count": 42
}
```

### GET /siem/offenses/{offense\_id}/notes DEPRECATED

Retrieve a list of notes for an offense.

Table 1141. GET /siem/offenses/{offense\_id}/notes resource details

MIME Type
application/json

Table 1142. GET /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the notes for.

Table 1142. GET /siem/offenses/{offense\_id}/notes request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1143. GET /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
200		The note list was retrieved.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the note list was being retrieved.

## Response Description

An array of Note objects. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
[
  {
    "create_time": 42,
    "id": 42,
```



```

    "note_text": "String",
    "username": "String"
  }
]

```

## POST /siem/offenses/{offense\_id}/notes DEPRECATED

Create a note on an offense.

Table 1144. POST /siem/offenses/{offense\_id}/notes resource details

MIME Type
application/json

Table 1145. POST /siem/offenses/{offense\_id}/notes request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to add the note to.
note_text	query	Required	String	text/plain	Required - The note text.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1146. POST /siem/offenses/{offense\_id}/notes response codes

HTTP Response Code	Unique Code	Description
201		The note was created.
404	1002	No offense was found for the provided offense_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create the note.

## Response Description

The Note object that was created. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.
- **note\_text** - String - The note text.

## Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## GET /siem/offenses/{offense\_id}/notes/{note\_id} DEPRECATED

Retrieve a note for an offense.

Table 1147. GET /siem/offenses/{offense\_id}/notes/{note\_id} resource details

MIME Type
application/json

Table 1148. GET /siem/offenses/{offense\_id}/notes/{note\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
offense_id	path	Required	Number (Integer)	text/plain	Required - The offense ID to retrieve the note from.
note_id	path	Required	Number (Integer)	text/plain	Required - The note ID.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1149. GET /siem/offenses/{offense\_id}/notes/{note\_id} response codes

HTTP Response Code	Unique Code	Description
200		The note was retrieved.
404	1002	No offense was found for the provided offense_id.
404	1003	No note was found for the provided note_id.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the note.

## Response Description

The Note object for the note ID. A Note object contains the following fields:

- **id** - Number - The ID of the note.
- **create\_time** - Number - The number of milliseconds since epoch when the note was created.
- **username** - String - The user or authorized service that created the note.

- **note\_text** - String - The note text.

### Response Sample

```
{
  "create_time": 42,
  "id": 42,
  "note_text": "String",
  "username": "String"
}
```

## REST API V2.0 References

Each API reference provides information about the parameters, mime type, stability, and responses for each endpoint.

### Ariel endpoints

Use the references for REST API V2 Ariel endpoints.

#### GET /ariel/databases DEPRECATED

Retrieve Ariel database names

Retrieve a list of available Ariel databases.

Table 1150. GET /ariel/databases resource details

MIME Type
application/json

Table 1151. GET /ariel/databases request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1152. GET /ariel/databases response codes

HTTP Response Code	Unique Code	Description
200		The database list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of Ariel databases.

## Response Description

The names of the available Ariel databases.

## Response Sample

```
[  
  "String"  
]
```

## GET /ariel/databases/{database\_name} DEPRECATED

This method has been deprecated and should no longer be used. It is replaced by v3.0 of the /databases/{database\_name} endpoint

Table 1153. GET /ariel/databases/{database\_name} resource details

MIME Type
application/json

Table 1154. GET /ariel/databases/{database\_name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
database_name	path	Required	String	text/plain	null
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1155. GET /ariel/databases/{database\_name} response codes

HTTP Response Code	Unique Code	Description
404	1002	null
422	1005	null
500	1020	null

## Response Description

### Response Sample

```
{
  "columns": [
    {
      "argument_type": "String <one of: OBJECT,
                        IP,
                        IPV_6,
                        NUMERIC,
                        METRIC,
                        TIME,
                        PORT,
                        STRING,
                        BOOLEAN,
                        GROUP,
                        QUICKSEARCH,
                        REFERENCE>",
      "calculated": true,
      "custom": true,
      "id": "String",
      "indexable": true,
      "label": "String"
    }
  ]
}
```

## GET /ariel/searches DEPRECATED

Retrieve Ariel search\_ids.

Retrieve the list of Ariel searches. This includes search\_ids for completed and active searches.

Table 1156. GET /ariel/searches resource details

MIME Type
application/json

Table 1157. GET /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1158. GET /ariel/searches response codes

HTTP Response Code	Unique Code	Description
200		The search list was retrieved.
500	1020	An error occurred while attempting to retrieve the list of searches.

## Response Description

A list of search IDs.

## Response Sample

```
[  
  "String"  
]
```

## POST /ariel/searches DEPRECATED

Create a new asynchronous Ariel search.

Create an Ariel search based on Ariel Query Language (AQL) query expressions. A `search_id` is returned with the search results. Searches are executed asynchronously. In subsequent API calls, you can use this `search_id` to determine the status of the search and retrieve the results.

This endpoint only accepts SELECT and RUN query expressions.

Queries are applied to the range of data in a certain time interval. By default this time interval is the last 60 seconds. An alternative time interval can be specified by providing values for the `start_time` and `end_time` parameters. These parameters are used to express an inclusive time range, each value is interpreted as the number of milliseconds since 0:00:00, January 1, 1970 UTC. If both `start_time` and `end_time` parameters are not provided, the query interval defaults to the last 60 seconds. Alternatively a time interval can be specified as part of the query expression, though the `start_time` and `end_time` parameters take precedence. For further information, see the AQL Reference Guide.

Table 1159. POST /ariel/searches resource details

MIME Type
application/json

Table 1160. POST /ariel/searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
query_expression	query	Required	String	text/plain	Required. The AQL query to execute.
search_id	query	Optional	String	text/plain	Optional. A <code>search_id</code> value to be used for the new search instead of a system generated <code>search_id</code> . The <code>search_id</code> must be unique and is only used for SELECT query expressions. The <code>search_id</code> can only contain numbers, letters, dashes and/or underscores.

Table 1160. POST /ariel/searches request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
start_time	query	Optional	Number (Integer)	text/plain	Optional. The beginning of the query time interval in milliseconds since 0:00:00 1/1/1970. This value takes precedence over query_expression. end_time must be specified for this value to be used.
end_time	query	Optional	Number (Integer)	text/plain	Optional. The end of the query time interval in milliseconds since 0:00:00 1/1/1970. This value takes precedence over query_expression. start_time must be specified for this value to be used.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1161. POST /ariel/searches response codes

HTTP Response Code	Unique Code	Description
201		An Ariel search was successfully created.
409	1004	The search could not be created, because the search_id is already in use. Use a unique search_id.
422	2000	The query_expression contains invalid AQL syntax.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create a search.

## Response Description

Information about the specified search, including the search\_id. Use the search\_id to access or manipulate the search with the other API endpoints.

If the search criteria matches the criteria of an existing search, the response message returns a reference to the original search\_id and a new search is not created.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## GET /ariel/searches/{search\_id} DEPRECATED

Retrieve information about an Ariel search

Retrieve status information for a search, based on the search\_id parameter. The same informational fields are returned regardless of whether the search is in progress or is complete.

Table 1162. GET /ariel/searches/{search\_id} resource details

MIME Type
application/json

Table 1163. GET /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The identifier for an Ariel search.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.



Table 1164. GET /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search information was retrieved.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to retrieve the search information.

## Response Description

Information about the specified search, including the search status.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## POST /ariel/searches/{search\_id} DEPRECATED

Update an Ariel search.

Update details for an Ariel search. You can update searches in the following ways:

- To cancel an active search, set the **status** parameter to CANCELED. This stops the search and keeps any search results that were collected before the search was canceled.
- The results for a completed search can be saved by setting the **save\_results** parameter to true. This ensures that the search is not automatically removed when it expires in accordance with the retention policy.

The Ariel server uses an internal retention policy to manage available disk space. Searches might be deleted automatically, according to the settings of the retention

policy. Searches with saved results are not automatically reclaimed by the server and are therefore retained. A search can be explicitly deleted by using the DELETE /searches/{search\_id} endpoint.

Note: Saving too many search results might result in insufficient disk space to process new searches.

Table 1165. POST /ariel/searches/{search\_id} resource details

<b>MIME Type</b>
application/json

Table 1166. POST /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The ID of the search to update.
save_results	query	Optional	String	text/plain	Optional. The only accepted value is true. If this value is provided, the search results will not be deleted by the search expiration removal process.
status	query	Optional	String	text/plain	Optional. The only accepted value is CANCELED. If this value is provided, the search will be canceled.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1167. POST /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
200		The search was updated.
404	1002	The search does not exist.
409	1008	The current status of the search prevented the search results from being saved.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to update the search.

## Response Description

Information about the specified search that was updated.

## Response Sample

```
{
  "compressed_data_file_count": 42,
  "compressed_data_total_size": 42,
  "cursor_id": "String",
  "data_file_count": 42,
  "data_total_size": 42,
  "desired_retention_time_msec": 42,
  "error_messages": [
    {
      "code": "String",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ],
  "index_file_count": 42,
  "index_total_size": 42,
  "processed_record_count": 42,
  "progress": 42,
  "query_execution_time": 42,
  "record_count": 42,
  "save_results": true,
  "search_id": "String",
  "status": "String <one of: WAIT, EXECUTE, SORTING, COMPLETED, CANCELED, ERROR>"
}
```

## DELETE /ariel/searches/{search\_id} DEPRECATED

Delete an Ariel search.

Deletes an Ariel search. This discards collected results and stops the search if it in progress. This search is deleted regardless of whether the results were saved.

Table 1168. DELETE /ariel/searches/{search\_id} resource details

<b>MIME Type</b>
application/json

Table 1169. DELETE /ariel/searches/{search\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	Required. The search_id of the search to delete.

Table 1170. DELETE /ariel/searches/{search\_id} response codes

HTTP Response Code	Unique Code	Description
204		The search was deleted.
404	1002	The search does not exist.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to delete the search.

## Response Description

There is no response body for a successfully deleted Ariel Search.

## Response Sample

```
{
  "error_messages": [
    {
      "code": "String <one of: ERROR_FILE_ACCESS,
              ERROR_CURSOR_CREATE,
              ERROR_CURSOR_CREATE_EXISTS,
              WARN_MAX_RECORDS,
              WARN_MAX_COLLECTED_RECORDS,
              ERROR_INVALID_CURSOR,
              ERROR_PROTECT_CURSOR,
              ERROR_SERVER_IO,
              WARN_INTERRUPT,
              ERROR_READ_TIMEOUT,
              ERROR_INVALID_QUERY_PARAMS,
              WARN_QUERY_TIME_LIMIT,
              ERROR_GENERAL_FAILURE,
              ERROR_FILE_RUNTIME_EXCEPTION,
              ERROR_INVALID_QUERY,
              WARN_CANCEL,
              INFO_INVALID_SORTING,
              ERROR_FETCH,
              WARN_SHARING_VIOLATION,
              WARN_INCOMPLETE_RESULT,
              ERROR_QUERY_EXPIRED,
              INFO_MAINTENANCE,
              ERROR_FUNCTION_ERROR,
              ERROR_COULD_NOT_CONNECT,
              ERROR_RB_COMMUNICATION,
              ERROR_RB_SOURCE_DATABLOCK_SEND,
              ERROR_RB_DESTINATION_DATABLOCK_RECEIVE,
              NEXUS_ERROR>",
      "contexts": [
        "String"
      ],
      "message": "String",
      "severity": "String <one of: INFO, WARN, ERROR>"
    }
  ]
}
```

## GET /ariel/searches/{search\_id}/results DEPRECATED

Retrieves search results in the requested format.

Retrieve the results of the Ariel search that is identified by the search\_id. The results are returned in the format that is indicated in the Accepts request header. The format can be JSON, CSV, XML, or tabular text.

By default, all query result records are returned. To restrict the results to a contiguous subset of the records, supply the range\_start and range\_end parameters.

This end-point works with query results that are generated by AQL query expressions, but it might not work as expected for results that are generated by other means. Search results might not be retrievable for searches that are created on the Console.

The response samples are for the following query: Select sourceIP, destinationIP from events

Table 1171. GET /ariel/searches/{search\_id}/results resource details

MIME Type
application/json application/csv text/table application/xml

Table 1172. GET /ariel/searches/{search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
search_id	path	Required	String	text/plain	The ID of the search whose results are to be returned.
range_start	query	Optional	Number (Integer)	text/plain	The first row of the range of records to return, starting from one (1).
range_end	query	Optional	Number (Integer)	text/plain	The last row of the range of records to be return.

Table 1173. GET /ariel/searches/{search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The search results were retrieved.
404	1002	The search does not exist.
404	1003	Search results were not found, because the search is still in progress.
422	1005	A request parameter is not valid.
422	1007	Retrieving the search results for this search_id is unsupported.
500	1020	An error occurred while attempting to retrieve the search results.

## Response Description

The search results for the specified search\_id. The format is specified in the Accept header for this request.

## Response Sample

```
{
  "events": [
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    },
    {
      "sourceIP": "1.1.1.1",
      "destinationIP": "127.0.0.1"
    }
  ]
}
```

## Asset Model endpoints

Use the references for REST API V2 Asset Model endpoints.

### GET /asset\_model/assets DEPRECATED

List all assets found in the model.

List all assets found in the model.

Table 1174. GET /asset\_model/assets resource details

MIME Type
application/json

Table 1175. GET /asset\_model/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1176. GET /asset\_model/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
500	1020	The server encountered an error while trying to retrieve the assets.

### Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[{"id": 42,
  "interfaces": [{"first_seen_scanner": 42,
    "id": 42,
    "first_seen_profiler": 42,
    "created": 42,
    "last_seen_profiler": 42,
    "last_seen_scanner": 42,
    "mac_address": "String",
    "ip_addresses": [{"first_seen_scanner": 42,
      "id": 42,
      "first_seen_profiler": 42,
      "created": 42,
      "network_id": 42,
      "value": "String",
      "last_seen_profiler": 42,
      "last_seen_scanner": 42,
      "type": "String"}]}],
  "properties": [{"id": 42,
    "name": "String",
    "value": "String",
    "last_reported": 42,
    "type_id": 42,
    "last_reported_by": "String"}]}]
```

## POST /asset\_model/assets/{asset\_id} DEPRECATED

Update an asset with several pertinent pieces of information.

Update an asset with several pertinent pieces of information. The **asset\_id** tag is mandatory, and is the unique identifier for an asset. This field is available through the `/asset_model/assets` or `/asset_model/saved_searches/{saved_search_id}/results` query. To update properties, the property type id which is available through the `/asset_model/properties` query should be provided along with the new value. See the sample provided demonstrating an example asset update.

Table 1177. POST /asset\_model/assets/{asset\_id} resource details

MIME Type
text/plain

Table 1178. POST /asset\_model/assets/{asset\_id} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
asset_id	path	Required	String	text/plain	Unique identifier of the asset to update.

Table 1179. POST /asset\_model/assets/{asset\_id} request body details

Parameter	Data Type	MIME Type	Description	Sample
asset	JSON	application/json	JSON representation of an asset.	{ "properties": [ { "type_id": 1001, "value": "given name value" }, { "type_id": 1002, "value": "unified name value" } ] }

Table 1180. POST /asset\_model/assets/{asset\_id} response codes

HTTP Response Code	Unique Code	Description
202		The request to update the asset was successful. The update will take place when the asset profile application receives the request.
422	1005	One or more of the requested property updates were invalid.
500	1020	The server encountered an error registering the update with the asset profile application.

## Response Description

Information about the asset that was updated.

## Response Sample

String

## GET /asset\_model/properties DEPRECATED

Get a list of available asset property types that can be used.

Get a list of available asset property types that can be used or applied against the /asset\_model/assets endpoint.

Table 1181. GET /asset\_model/properties resource details

MIME Type
application/json

Table 1182. GET /asset\_model/properties request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.



Table 1182. GET /asset\_model/properties request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1183. GET /asset\_model/properties response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of asset property types completed successfully.
500	1020	An error occurred while trying to retrieve the list of asset property types.

## Response Description

List of asset properties. Per asset property type: id and name that make up this asset property type.

## Response Sample

```
[
  {
    "custom": true,
    "data_type": "String",
    "display": true,
    "id": 42,
    "name": "String",
    "state": 42
  }
]
```

## GET /asset\_model/saved\_searches DEPRECATED

Get a list of saved searches that can be used.

Get a list of saved searches that can be used or applied against the `/asset_model/saved_searches/{saved_search_id}/results` query.

Table 1184. GET /asset\_model/saved\_searches resource details

MIME Type
application/json

Table 1185. GET /asset\_model/saved\_searches request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1186. GET /asset\_model/saved\_searches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully.
500	1020	The server encountered an error while trying to retrieve the list of saved searches.

## Response Description

List of saved searches. Per saved search: id, name and list of filters that make up this saved search

## Response Sample

```
[
  {
    "columns": [
      {
        "name": "String",
        "type": "String"
      }
    ],
    "description": "String",
    "filters": [
      {
        "operator": "String",
        "parameter": "String",
        "value": "String"
      }
    ]
  }
]
```

```

    },
    "id": 42,
    "name": "String"
  }
]

```

## GET /asset\_model/saved\_searches/{saved\_search\_id}/results DEPRECATED

Retrieves a list of assets based on the results of an asset saved search.

Retrieves a list of assets based on the results of an asset saved search.

Table 1187. GET /asset\_model/saved\_searches/{saved\_search\_id}/results resource details

MIME Type
application/json

Table 1188. GET /asset\_model/saved\_searches/{saved\_search\_id}/results request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
saved_search_id	path	Required	String	text/plain	Unique identifier of the saved search used to retrieve assets.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1189. GET /asset\_model/saved\_searches/{saved\_search\_id}/results response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve assets completed successfully.
422	1005	The unique identifier of the saved search provided was invalid.
500	1003	The server encountered an error executing the saved search.

## Response Description

List of assets retrieved using the associated asset saved search.

## Response Sample

```
[
  {
    "id": 42,
    "interfaces": [
      {
        "created": 42,
        "first_seen_profiler": 42,
        "first_seen_scanner": 42,
        "id": 42,
        "ip_addresses": [
          {
            "created": 42,
            "first_seen_profiler": 42,
            "first_seen_scanner": 42,
            "id": 42,
            "last_seen_profiler": 42,
            "last_seen_scanner": 42,
            "network_id": 42,
            "type": "String",
            "value": "String"
          }
        ],
        "last_seen_profiler": 42,
        "last_seen_scanner": 42,
        "mac_address": "String"
      }
    ],
    "properties": [
      {
        "id": 42,
        "last_reported": 42,
        "last_reported_by": "String",
        "name": "String",
        "type_id": 42,
        "value": "String"
      }
    ]
  }
]
```

## Authentication endpoints

Use the references for REST API V2 authentication endpoints.

### POST /auth/logout DEPRECATED

Invoke this method as an authorized user and your session will be invalidated.

Table 1190. POST /auth/logout resource details

MIME Type
text/plain

There are no parameters for this endpoint.

Table 1191. POST /auth/logout response codes

HTTP Response Code	Unique Code	Description
200		The session was invalidated.

## Response Description

Returns true. Throws exception upon failure.

## Response Sample

```
true
```

## Help endpoints

Use the references for REST API V3.1 Help endpoints.

### GET /help/capabilities DEPRECATED

List all QRadar API capabilities

List the QRadar API capabilities. The response will contain all available RESTful resources We allow every authenticated user to access this method, but restrict the output based on their user capabilities

Table 1192. GET /help/capabilities resource details

MIME Type
application/json

Table 1193. GET /help/capabilities request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
categories	query	Optional	Array<String>	application/json	Optional - Restrict your search to this list of capabilities
paths	query	Optional	Array<String>	application/json	Optional - Restrict your search to these paths only
httpMethods	query	Optional	Array<String>	application/json	Optional - Restrict your search to these HTTP methods
version	query	Optional	String	text/plain	Optional - Restrict your search to this version (or below)
showExperimental	query	Optional	Boolean	text/plain	Optional - If true, we include experimental endpoints (default is true)
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1194. GET /help/capabilities response codes

HTTP Response Code	Unique Code	Description
200		The API capabilities list was retrieved.
422	1001	Invalid input
422	1002	Our internal mapping has an unexpected structure or contains an invalid element value
500	1003	A generic error has occurred while retrieving our capabilities

## Response Description

Endpoints you are able to access, mapped against versions they belong to. If full content is not requested, values will be null.

## Response Sample

```
{
  "categories": [
    {
      "apis": [
        {
          "httpMethod": "String <one of: OPTIONS,
            GET,
            HEAD,
            POST,
            PUT,
            DELETE,
            TRACE,
            CONNECT,
            PATCH>",
          "operations": [
            {
              "additionalFiltering": true,
              "deprecated": true,
              "description": "String",
              "errorResponses": [
                {
                  "code": 42,
                  "description": "String",
                  "uniqueCode": 42
                }
              ],
              "httpMethod": "String",
              "lastSupportedVersion": "String",
              "parameters": [
                {
                  "allowMultiple": true,
                  "defaultValue": "String",
                  "description": "String",
                  "name": "String",
                  "pathIndex": 42,
                  "required": true,
                  "source": "String",
                  "supportedContentTypes": [
                    {
                      "dataType": "String",
                      "mimeType": "String",
                      "sample": "String"
                    }
                  ]
                }
              ]
            }
          ]
        }
      ]
    }
  ]
}
```

```

    ],
    "removalTarget": "String",
    "removed": true,
    "responseClass": "String",
    "responseDescription": {
      "description": "String",
      "properties": [
        {
          "description": "String",
          "name": "String"
        }
      ]
    },
    "successResponses": [
      {
        "code": 42,
        "description": "String"
      }
    ],
    "summary": "String",
    "supportedContentTypes": [
      {
        "dataType": "String",
        "mimeType": "String",
        "sample": "String"
      }
    ],
    "version": "String",
    "visibility": "String"
  },
  "path": "String"
},
"path": "String"
},
"path": "String"
}

```

## QRadar Vulnerability Manager endpoints

Use the references for REST API V2 QRadar Vulnerability Manager endpoints.

### GET /qvm/assets DEPRECATED

List the assets with discovered vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 1195. GET /qvm/assets resource details

MIME Type
application/json

Table 1196. GET /qvm/assets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name

Table 1196. GET /qvm/assets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 1197. GET /qvm/assets response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by asset completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of assets data

## Response Sample

### GET /qvm/filters DEPRECATED

Get a list of the allowable filters that can be used or applied against /qvm endpoints:

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 1198. GET /qvm/filters resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 1199. GET /qvm/filters response codes

HTTP Response Code	Unique Code	Description
200		The search executed successfully
420	9102	An error occurred while executing the search

## Response Description

list of Filters.



## Response Sample

### GET /qvm/network DEPRECATED

List the networks present in the asset model with vulnerabilities present. The response will contain all available RESTful resources

Table 1200. GET /qvm/network resource details

<b>MIME Type</b>
application/json

Table 1201. GET /qvm/network request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 1202. GET /qvm/network response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by network completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

List of network related data.

## Response Sample

### GET /qvm/openservices DEPRECATED

List the openservices present in the asset model with vulnerabilities present. The response will contain all available RESTful resources

Table 1203. GET /qvm/openservices resource details

<b>MIME Type</b>
application/json

Table 1204. GET /qvm/openservices request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name

Table 1204. GET /qvm/openservices request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 1205. GET /qvm/openservices response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by open service completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of open services related data

## Response Sample

### GET /qvm/savedsearches DEPRECATED

Get a list of saved searches that can be applied against /qvm endpoints.

A list of saved searches that can be applied against the following endpoints:

- /qvm/assets
- /qvm/vulns
- /qvm/vulninstances
- /qvm/openservices
- /qvm/networks
- queries

Table 1206. GET /qvm/savedsearches resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 1207. GET /qvm/savedsearches response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve the list of saved searches completed successfully
420	9103	An error occurred while trying to retrieve the list of saved searches

## Response Description

list of saved searches. Per saved search: id, name and list fo filters that make up this saved search

## Response Sample

### POST /qvm/tickets/assign DEPRECATED

Update the remediation ticket for the assigned vulnerability

Table 1208. POST /qvm/tickets/assign resource details

<b>MIME Type</b>
application/json

Table 1209. POST /qvm/tickets/assign request body details

Parameter	Data Type	MIME Type	Description	Sample
ticket	JSON	application/json	'ticketId': required.  'priority' one of required : Critical, Major, Minor, Warning, Informational.  'status' one of required : Opened, Fixed, Re-Opened, Closed .  'dueDate' Optional : yyyy-MM-dd HH:mm:ss.  'assignedUser' required : valid QRadar user account name or a valid email.  'comment' Optional : text.  'commentUser' Optional : valid QRadar user account name, if not included will default current API user.	[ { "ticketId": "1000", "status": "Opened", "priority": "Critical", "dueDate": "2015-01-04 12:00:00", "assignedUser": "admin", "comment": "testComment", "commentUser": "admin" } ]

Table 1210. POST /qvm/tickets/assign response codes

HTTP Response Code	Unique Code	Description
200		The request to assign a ticket completed successfully
420	9104	An error occurred while trying to assign a ticket due to invalid arguments

## Response Description

Success message if update succeed

## Response Sample

### GET /qvm/vulninstances DEPRECATED

List the Vulnerability Instances present in the asset model. The response will contain all available RESTful resources.

Table 1211. GET /qvm/vulninstances resource details

<b>MIME Type</b>
application/json

Table 1212. GET /qvm/vulninstances request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 1213. GET /qvm/vulninstances response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities by instance completed successfully.
420	9101	Invalid search parameters, search cannot be performed.

## Response Description

List of vulnerability instance data.

## Response Sample

### GET /qvm/vulns DEPRECATED

List the Vulnerabilities present in the asset model. The response will contain all available RESTful resources

Table 1214. GET /qvm/vulns resource details

MIME Type
application/json

Table 1215. GET /qvm/vulns request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
savedSearchId	query	Optional	String	text/plain	Id of saved search
savedSearchName	query	Optional	String	text/plain	Saved search name
filters	query	Optional	Array<Object>	application/json	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter": "<value>", "operator": "<value>", "value": "<value>"}] e.g. [{"parameter": "IPv4 Address", "operator": "Equals", "value": "10.100.85.111"}]

Table 1216. GET /qvm/vulns response codes

HTTP Response Code	Unique Code	Description
200		The request to retrieve vulnerabilities completed successfully
420	9101	Invalid search parameters, search cannot be performed

## Response Description

list of vulnerability data

## Response Sample

## Reference Data endpoints

Use the references for REST API V2 Reference Data endpoints.

### GET /reference\_data/map\_of\_sets DEPRECATED

Retrieve a list of all reference map of sets.

Retrieve a list of all reference map of sets.

Table 1217. GET /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 1218. GET /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1219. GET /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

## Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## POST /reference\_data/map\_of\_sets DEPRECATED

Create a new reference map of sets.

Create a new reference map of sets.

Table 1220. POST /reference\_data/map\_of\_sets resource details

MIME Type
application/json

Table 1221. POST /reference\_data/map\_of\_sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values

Table 1221. POST /reference\_data/map\_of\_sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1222. POST /reference\_data/map\_of\_sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/map\_of\_sets/{name} DEPRECATED

Return the reference map of sets identified by name.

Return the reference map of sets identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1223. GET /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 1224. GET /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map of sets. The default value is 0.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1225. GET /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map of sets



## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": [
      {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    ]
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/map\_of\_sets/{name} DEPRECATED

Add or update an element in a reference map of sets.

Add or update an element in a reference map of sets.

Table 1226. POST /reference\_data/map\_of\_sets/{name} resource details

MIME Type
application/json

Table 1227. POST /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1227. POST /reference\_data/map\_of\_sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1228. POST /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map of sets

## Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name} DEPRECATED

Remove a map of sets or purge its contents.

Remove a map of sets or purge its contents.

Table 1229. DELETE /reference\_data/map\_of\_sets/{name} resource details

<b>MIME Type</b>
application/json

Table 1230. DELETE /reference\_data/map\_of\_sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1231. DELETE /reference\_data/map\_of\_sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map of sets does not exist
409	1004	The reference map of sets could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

## Response Description

If the reference map of sets was removed nothing is returned, otherwise information about the reference map of sets that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/map\_of\_sets/{name}/{key} DEPRECATED

Remove a value from a reference map of sets.

Remove a value from a reference map of sets.

Table 1232. DELETE /reference\_data/map\_of\_sets/{name}/{key} resource details

MIME Type
application/json

Table 1233. DELETE /reference\_data/map\_of\_sets/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1234. DELETE /reference\_data/map\_of\_sets/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

## Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps DEPRECATED

Retrieve a list of all reference maps.

Retrieve a list of all reference maps.

Table 1235. GET /reference\_data/maps resource details

MIME Type
application/json

Table 1236. GET /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1236. GET /reference\_data/maps request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1237. GET /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

## Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "value_label": "String"
  }
]
```

## POST /reference\_data/maps DEPRECATED

Create a new reference map.

Create a new reference map.

Table 1238. POST /reference\_data/maps resource details

MIME Type
application/json

Table 1239. POST /reference\_data/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create

Table 1239. POST /reference\_data/maps request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
key_label	query	Optional	String	text/plain	Optional - The label to describe the keys
value_label	query	Optional	String	text/plain	Optional - The label to describe the data values
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1240. POST /reference\_data/maps response codes

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid

Table 1240. *POST /reference\_data/maps* response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/maps/{name} DEPRECATED

Retrieve the reference map identified by name.

Retrieve the reference map identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1241. *GET /reference\_data/maps/{name}* resource details

MIME Type
application/json

Table 1242. *GET /reference\_data/maps/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map. The default value is 0.



Table 1242. GET /reference\_data/maps/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1243. GET /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## POST /reference\_data/maps/{name} DEPRECATED

Add or update an element in a reference map.

Add or update an element in a reference map.

Table 1244. POST /reference\_data/maps/{name} resource details

<b>MIME Type</b>
application/json

Table 1245. POST /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1246. POST /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## DELETE /reference\_data/maps/{name} DEPRECATED

Remove a reference map or purge its contents.

Remove a reference map or purge its contents.

Table 1247. DELETE /reference\_data/maps/{name} resource details

MIME Type
application/json

Table 1248. DELETE /reference\_data/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1249. DELETE /reference\_data/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map does not exist
409	1004	The reference map could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

### Response Description

If the reference map was removed nothing is returned, otherwise information about the reference map that had its contents purged is returned.

### Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

### DELETE /reference\_data/maps/{name}/{key} DEPRECATED

Remove a value from a reference map.

Remove a value from a reference map.

Table 1250. DELETE /reference\_data/maps/{name}/{key} resource details

MIME Type
application/json

Table 1251. DELETE /reference\_data/maps/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove

Table 1251. DELETE /reference\_data/maps/{name}/{key} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1252. DELETE /reference\_data/maps/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

## Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "value_label": "String"
}
```

## GET /reference\_data/sets DEPRECATED

Retrieve a list of all reference sets.

Retrieve a list of all reference sets.

Table 1253. GET /reference\_data/sets resource details

<b>MIME Type</b>
application/json

Table 1254. GET /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1255. GET /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

## Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## POST /reference\_data/sets DEPRECATED

Create a new reference set.

Create a new reference set.

Table 1256. POST /reference\_data/sets resource details

MIME Type
application/json

Table 1257. POST /reference\_data/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created
element_type	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1258. POST /reference\_data/sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/sets/{name} DEPRECATED

Retrieve the reference set identified by name.

Retrieve the reference set identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1259. GET /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 1260. GET /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference set. The default value is 0.



Table 1260. GET /reference\_data/sets/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1261. GET /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": [
    {
      "first_seen": 42,
      "last_seen": 42,
      "source": "String",
      "value": "String"
    }
  ],
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/{name} DEPRECATED

Add or update an element in a reference set.

Add or update an element in a reference set.

Table 1262. POST /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 1263. POST /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1264. POST /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update an element in the reference set

## Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
```

```

    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## DELETE /reference\_data/sets/{name} DEPRECATED

Remove a reference set or purge its contents.

Remove a reference set or purge its contents.

Table 1265. DELETE /reference\_data/sets/{name} resource details

MIME Type
application/json

Table 1266. DELETE /reference\_data/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1267. DELETE /reference\_data/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had its contents purged
204		The reference set has been removed
404	1002	The reference set does not exist
409	1004	The reference set could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid

Table 1267. DELETE /reference\_data/sets/{name} response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to remove or purge values from the reference set

## Response Description

If the reference set was removed nothing is returned, otherwise information about the reference set that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/sets/{name}/{value} DEPRECATED

Remove a value from a reference set.

Remove a value from a reference set.

Table 1268. DELETE /reference\_data/sets/{name}/{value} resource details

MIME Type
application/json

Table 1269. DELETE /reference\_data/sets/{name}/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1270. DELETE /reference\_data/sets/{name}/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had an value removed. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## POST /reference\_data/sets/bulk\_load/{name} DEPRECATED

Add or update data in a reference set.

Add or update data in a reference set.

Table 1271. POST /reference\_data/sets/bulk\_load/{name} resource details

MIME Type
application/json

Table 1272. POST /reference\_data/sets/bulk\_load/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in
fields	header	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1273. POST /reference\_data/sets/bulk\_load/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Array	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 1274. POST /reference\_data/sets/bulk\_load/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

## Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables DEPRECATED

Retrieve a list of all reference tables.

Retrieve a list of all reference tables.

Table 1275. GET /reference\_data/tables resource details

MIME Type
application/json

Table 1276. GET /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1277. GET /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```
[
  {
    "creation_time": 42,
    "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "key_label": "String",
    "key_name_types": {
      "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
    },
    "name": "String",
    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]
```

## POST /reference\_data/tables DEPRECATED

Create a new reference table.

Create a new reference table.

Table 1278. POST /reference\_data/tables resource details

MIME Type
application/json

Table 1279. POST /reference\_data/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create
element_type	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>key_name_types</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outer_key_label	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeout_type	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the time_to_live interval is based on when the data was first seen or last seen.
time_to_live	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
key_name_types	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.



Table 1280. POST /reference\_data/tables response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /reference\_data/tables/{name} DEPRECATED

Return the reference table identified by name.

Return the reference table identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1281. GET /reference\_data/tables/{name} resource details

MIME Type
application/json

Table 1282. GET /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.

Table 1282. GET /reference\_data/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference table. The default value is 0.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1283. GET /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "creation_time": 42,
  "data": {
    "String": {
      "String": {
        "first_seen": 42,
        "last_seen": 42,
        "source": "String",
        "value": "String"
      }
    }
  },
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
}
```

```

"name": "String",
"number_of_elements": 42,
"time_to_live": "String",
"timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## POST /reference\_data/tables/{name} DEPRECATED

Add or update an element in a reference table.

Add or update an element in a reference table. The value to be added must be of the appropriate type: either the type that corresponds to the innerKey predefined for the reference table, or the default elementType of the reference table

Table 1284. POST /reference\_data/tables/{name} resource details

MIME Type
application/json

Table 1285. POST /reference\_data/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to add or update an element in
outer_key	query	Required	String	text/plain	Required - The outer key for the element to add or update
inner_key	query	Required	String	text/plain	Required - The inner key for the element to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1286. *POST /reference\_data/tables/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table

## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## DELETE /reference\_data/tables/{name} DEPRECATED

Remove a reference table or purge its contents.

Remove a reference table or purge its contents.

Table 1287. *DELETE /reference\_data/tables/{name}* resource details

MIME Type
application/json

Table 1288. *DELETE /reference\_data/tables/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge

Table 1288. DELETE /reference\_data/tables/{name} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
purge_only	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1289. DELETE /reference\_data/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had its contents purged
204		The reference table has been removed
404	1002	The reference table does not exist
409	1004	The reference table could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

## Response Description

If the table was removed nothing is returned, otherwise information about the reference table that had its contents purged is returned.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
```

```

    "number_of_elements": 42,
    "time_to_live": "String",
    "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}

```

## DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} DEPRECATED

Remove a value from a reference table.

Remove a value from a reference table.

Table 1290. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} resource details

MIME Type
application/json

Table 1291. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from
outer_key	path	Required	String	text/plain	Required - The outer key of the value to remove
inner_key	path	Required	String	text/plain	Required - The inner key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1292. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table

Table 1292. DELETE /reference\_data/tables/{name}/{outer\_key}/{inner\_key} response codes (continued)

HTTP Response Code	Unique Code	Description
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference table value

## Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

## Response Sample

```
{
  "creation_time": 42,
  "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "key_label": "String",
  "key_name_types": {
    "String": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  },
  "name": "String",
  "number_of_elements": 42,
  "time_to_live": "String",
  "timeout_type": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
}
```

## GET /referencedata/mapOfSets DEPRECATED

Retrieve a list of all reference map of sets

Table 1293. GET /referencedata/mapOfSets resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 1294. GET /referencedata/mapOfSets response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference map of sets

## Response Description

A list of all of the reference map of sets. This returns information about the map of sets but not the contained data.

## Response Sample

```
[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398377702319,
  }
]
```

```

"timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"valueLabel": "String",
"numberOfElements": 42
},
{
"name": "String",
"elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
"createdTime": 1398377702319,
"timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"valueLabel": "String",
"numberOfElements": 42
},
{
"name": "String",
"elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
"createdTime": 1398377702319,
"timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"valueLabel": "String",
"numberOfElements": 42
}
]

```

## POST /referencedata/mapOfSets DEPRECATED

Create a new reference map of sets

Table 1295. POST /referencedata/mapOfSets resource details

<b>MIME Type</b>
application/json

Table 1296. POST /referencedata/mapOfSets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map of sets to create
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map of sets. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
keyLabel	query	Optional	String	text/plain	Optional - The label to describe the keys
valueLabel	query	Optional	String	text/plain	Optional - The label to describe the data values



Table 1296. POST /referencedata/mapOfSets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 1297. POST /referencedata/mapOfSets response codes

HTTP Response Code	Unique Code	Description
201		A new reference map of sets was successfully created
409	1004	The reference map of sets could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map of sets

## Response Description

Information about the newly created reference map of sets.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## GET /referencedata/mapOfSets/{name} DEPRECATED

Return the reference map of sets identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1298. GET /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 1299. GET /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map of sets. The default value is 0.

Table 1300. GET /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has been retrieved
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map of sets

## Response Description

The reference map of sets identified by the name specified in the request. The portion of the reference map of sets' data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 9,
  "data": {
    "String1": [
      {
        "value": "String",
        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
      },
      {
        "value": "String",
        "source": "String",
        "firstSeen": 1398377702319,
        "lastSeen": 1398377702319
      }
    ]
  }
}
```

```

    },
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    }
  ],
  "String2": [
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    },
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    },
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    }
  ],
  "String3": [
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    },
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    },
    {
      "value": "String",
      "source": "String",
      "firstSeen": 1398377702319,
      "lastSeen": 1398377702319
    }
  ]
}

```

## POST /referencedata/mapOfSets/{name} DEPRECATED

Add or update an element in a reference map of sets

Table 1301. POST /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 1302. POST /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to add or update an element in
key	query	Required	String	text/plain	Required - The key of the set to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - This indicates where the data originated. The default value is 'reference data api'

Table 1303. POST /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had an element added or updated
404	1002	The reference map of sets does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map of sets

## Response Description

Information about the reference map of sets that has had an element added or updated. This returns information about the reference map of sets but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## DELETE /referencedata/mapOfSets/{name} DEPRECATED

Remove a map of sets or purge its contents

Table 1304. DELETE /referencedata/mapOfSets/{name} resource details

MIME Type
application/json

Table 1305. DELETE /referencedata/mapOfSets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map of sets should have its contents purged (true), keeping the reference map of sets structure. If the value is "false" or not specified the reference map of sets will be removed completely.

Table 1306. DELETE /referencedata/mapOfSets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map of sets does not exist
409	1004	The reference map of sets could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map of sets

### Response Description

If the reference map of sets was removed nothing is returned, otherwise information about the reference map of sets that had its contents purged is returned.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
```

```

"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"valueLabel": "String",
"numberOfElements": 0
}

```

## DELETE /referencedata/mapOfSets/{name}/{key} DEPRECATED

Remove a value from a reference map of sets

Table 1307. DELETE /referencedata/mapOfSets/{name}/{key} resource details

<b>MIME Type</b>
application/json

Table 1308. DELETE /referencedata/mapOfSets/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map of sets to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map of sets. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1309. DELETE /referencedata/mapOfSets/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map of sets has had a value removed
404	1002	The reference map of sets does not exist
404	1003	The record does not exist in the reference map of sets
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the reference map of sets value

### Response Description

Information about the reference map of sets that had a value removed. This returns information about the reference map of sets but not the contained data.

### Response Sample

```

{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398377702319,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",

```

```

    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
    "valueLabel": "String",
    "numberOfElements": 5
}

```

## GET /referencedata/maps DEPRECATED

Retrieve a list of all reference maps

Table 1310. GET /referencedata/maps resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 1311. GET /referencedata/maps response codes

HTTP Response Code	Unique Code	Description
200		The reference map list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference maps

## Response Description

A list of all of the reference maps. This returns information about the maps but not the contained data.

## Response Sample

```

[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
    "valueLabel": "String",
    "numberOfElements": 42
  },
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 1398265631810,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
    "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
    "key1Label": "String",
  }
]

```

```

    "valueLabel": "String",
    "numberOfElements": 42
  }
]

```

## POST /referencedata/maps DEPRECATED

Create a new reference map

Table 1312. POST /referencedata/maps resource details

<b>MIME Type</b>
application/json

Table 1313. POST /referencedata/maps request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference map to create
keyLabel	query	Optional	String	text/plain	Optional - The label to describe the keys
valueLabel	query	Optional	String	text/plain	Optional - The label to describe the data values
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference map. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 1314. POST /referencedata/maps response codes

HTTP Response Code	Unique Code	Description
201		A new reference map was successfully created



Table 1314. *POST /referencedata/maps* response codes (continued)

HTTP Response Code	Unique Code	Description
409	1004	The reference map could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference map

## Response Description

Information about the newly created reference map.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "valueLabel": "String",
  "numberOfElements": 0
}
```

## GET /referencedata/maps/{name} DEPRECATED

Retrieve the reference map identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1315. *GET /referencedata/maps/{name}* resource details

MIME Type
application/json

Table 1316. *GET /referencedata/maps/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference map. The default value is 0.

Table 1317. GET /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has been retrieved
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference map

## Response Description

The reference map identified by the name specified in the request. The portion of the reference map's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1396355660000,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "valueLabel": "String",
  "numberOfElements": 3,
  "data": {
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    },
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    },
    "String": {
      "value": "String",
      "source": "String",
      "firstSeen": 1396355660001,
      "lastSeen": 1396355660001
    }
  }
}
```

## POST /referencedata/maps/{name} DEPRECATED

Add or update an element in a reference map

Table 1318. POST /referencedata/maps/{name} resource details

MIME Type
application/json

Table 1319. POST /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to add or update an element in
key	query	Required	String	text/plain	Required - The key who's value we want to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 1320. POST /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had an element added or updated
404	1002	The reference map does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference map

## Response Description

Information about the reference map that had an element added or updated. This returns information about reference map but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "valueLabel": "String",
  "numberOfElements": 5
}
```

## DELETE /referencedata/maps/{name} DEPRECATED

Remove a reference map or purge its contents

Table 1321. DELETE /referencedata/maps/{name} resource details

MIME Type
application/json

Table 1322. DELETE /referencedata/maps/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference map should have its contents purged (true), keeping the reference map structure. If the value is "false" or not specified the reference map will be removed completely.

Table 1323. DELETE /referencedata/maps/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had its contents purged
204		The reference map has been removed
404	1002	The reference map does not exist
409	1004	The reference map could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference map

### Response Description

If the reference map was removed nothing is returned, otherwise information about the reference map that had its contents purged is returned.

### Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
```

```

    "keyLabel": "String",
    "valueLabel": "String",
    "numberOfElements": 0
}

```

## DELETE /referencedata/maps/{name}/{key} DEPRECATED

Remove a value from a reference map

Table 1324. DELETE /referencedata/maps/{name}/{key} resource details

MIME Type
application/json

Table 1325. DELETE /referencedata/maps/{name}/{key} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference map to remove a value from
key	path	Required	String	text/plain	Required - The key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference map. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1326. DELETE /referencedata/maps/{name}/{key} response codes

HTTP Response Code	Unique Code	Description
200		The reference map has had a value removed
404	1002	The reference map does not exist
404	1003	The record does not exist in the reference map
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference map

## Response Description

Information about the reference map that had an element removed. This returns information about map but not the contained data.

## Response Sample

```

{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398265631810,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
}

```

```

    "key1Label": "String",
    "valueLabel": "String",
    "numberOfElements": 5
}

```

## GET /referencedata/sets DEPRECATED

Retrieve a list of all reference sets.

Table 1327. GET /referencedata/sets resource details

<b>MIME Type</b>
application/json

There are no parameters for this endpoint.

Table 1328. GET /referencedata/sets response codes

HTTP Response Code	Unique Code	Description
200		The reference set list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference sets

## Response Description

A list of all of the reference sets. This returns information about the sets but not the contained data.

## Response Sample

```

[
  {
    "creationTime": 42,
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "name": "String",
    "numberOfElements": 42,
    "timeToLive": "String",
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>"
  }
]

```

## POST /referencedata/sets DEPRECATED

Create a new reference set

Table 1329. POST /referencedata/sets resource details

<b>MIME Type</b>
application/json

Table 1330. POST /referencedata/sets request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference set being created

Table 1330. POST /referencedata/sets request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
elementType	query	Required	String	text/plain	Required - The element type for the values allowed in the reference set. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the timeToLive interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"

Table 1331. POST /referencedata/sets response codes

HTTP Response Code	Unique Code	Description
201		A new reference set was successfully created
409	1004	The reference set could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference set

## Response Description

Information about the newly created reference set.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398777706999,
```

```

"timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"numberOfElements": 0
}

```

## GET /referencedata/sets/{name} DEPRECATED

Retrieve the reference set identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1332. GET /referencedata/sets/{name} resource details

<b>MIME Type</b>
application/json

Table 1333. GET /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference set. The default value is 0.

Table 1334. GET /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has been retrieved
404	1002	The reference set does not exist.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference set

## Response Description

The reference set identified by the name specified in the request. The portion of the set's data returned is dependent on the limit and offset specified in the request.

## Response Sample

```

{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1398277745579,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 3,
}

```



```

"data": [
  {
    "value": "String",
    "source": "String",
    "firstSeen": 1398277745579,
    "lastSeen": 1398277745579
  },
  {
    "value": "String",
    "source": "String",
    "firstSeen": 1398277745579,
    "lastSeen": 1398277745579
  },
  {
    "value": "String",
    "source": "String",
    "firstSeen": 1398277745579,
    "lastSeen": 1398277745579
  }
]
}

```

## POST /referencedata/sets/{name} DEPRECATED

Add or update an element in a reference set

Table 1335. POST /referencedata/sets/{name} resource details

MIME Type
application/json

Table 1336. POST /referencedata/sets/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to add or update an element in
value	query	Required	String	text/plain	Required - The value to add or update in the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 1337. POST /referencedata/sets/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had an element added or updated
404	1002	The reference set does not exist
422	1005	A request parameter is not valid

Table 1337. *POST /referencedata/sets/{name}* response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to add or update an element in the reference set

## Response Description

Information about the reference set that had an element added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 5
}
```

## DELETE /referencedata/sets/{name} DEPRECATED

Remove a reference set or purge its contents

Table 1338. *DELETE /referencedata/sets/{name}* resource details

MIME Type
application/json

Table 1339. *DELETE /referencedata/sets/{name}* request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the set to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference set should have its contents purged (true), keeping the reference set structure. If the value is "false" or not specified the reference set will be removed completely.

Table 1340. *DELETE /referencedata/sets/{name}* response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had its contents purged
204		The reference set has been removed

Table 1340. DELETE /referencedata/sets/{name} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1002	The reference set does not exist
409	1004	The reference set could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference set

## Response Description

If the reference set was removed nothing is returned, otherwise information about the reference set that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 0
}
```

## DELETE /referencedata/sets/{name}/{value} DEPRECATED

Remove a value from a reference set

Table 1341. DELETE /referencedata/sets/{name}/{value} resource details

MIME Type
application/json

Table 1342. DELETE /referencedata/sets/{name}/{value} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference set to remove a value from
value	path	Required	String	text/plain	Required - The value to remove from the reference set. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1343. DELETE /referencedata/sets/{name}/{value} response codes

HTTP Response Code	Unique Code	Description
200		The reference set that had a value removed
404	1002	The reference set does not exist

Table 1343. DELETE /referencedata/sets/{name}/{value} response codes (continued)

HTTP Response Code	Unique Code	Description
404	1003	The record does not exist in the reference set
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove the value from the reference set.

## Response Description

Information about the reference set that had an value removed. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 5
}
```

## POST /referencedata/sets/bulkLoad/{name} DEPRECATED

Add or update data in a reference set

Table 1344. POST /referencedata/sets/bulkLoad/{name} resource details

MIME Type
application/json

Table 1345. POST /referencedata/sets/bulkLoad/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of set to add or update data in

Table 1346. POST /referencedata/sets/bulkLoad/{name} request body details

Parameter	Data Type	MIME Type	Description	Sample
data	Object	application/json	Required - The JSON formatted data to add or update in the reference set	["String", "String", "String", "String", "String", "String", "String", "String", "String"]

Table 1347. POST /referencedata/sets/bulkLoad/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference set has had data added or updated

Table 1347. *POST /referencedata/sets/bulkLoad/{name}* response codes (continued)

HTTP Response Code	Unique Code	Description
400	1001	An error occurred parsing the JSON formatted message body
404	1002	The reference set does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference set

## Response Description

Information about the reference set that had data added or updated. This returns information about the reference set but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 139877706999,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "numberOfElements": 0
}
```

## GET /referencedata/tables DEPRECATED

Retrieve a list of all reference tables

Table 1348. *GET /referencedata/tables* resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 1349. *GET /referencedata/tables* response codes

HTTP Response Code	Unique Code	Description
200		The reference table list has been retrieved
500	1020	An error occurred while attempting to retrieve all of the reference tables

## Response Description

A list of all of the reference tables. This returns information about the tables but not the contained data.

## Response Sample

```
[
  {
    "name": "String",
    "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "createdTime": 139773789254,
    "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
```

```

"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"keyLabel": "String",
"numberOfElements": 42,
"keyNameTypes": {
  "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
}
},
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "numberOfElements": 42,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
},
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "keyLabel": "String",
  "numberOfElements": 42,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
]

```

## POST /referencedata/tables DEPRECATED

Create a new reference table

Table 1350. POST /referencedata/tables resource details

<b>MIME Type</b>
application/json

Table 1351. POST /referencedata/tables request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	query	Required	String	text/plain	Required - The name of the reference table to create

Table 1351. POST /referencedata/tables request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
elementType	query	Required	String	text/plain	Required - The default element type for the values allowed in the reference table. This is used when values are added or updated in the reference table who's inner key was not defined in the <b>keyNameTypes</b> parameter. The allowed values are: ALN (alphanumeric), ALNIC (alphanumeric ignore case), IP (IP address), NUM (numeric), PORT (port number) or DATE. Note that date values need to be represented in milliseconds since the Unix Epoch January 1st 1970.
outerKeyLabel	query	Optional	String	text/plain	Optional - The label to describe the outer keys
timeoutType	query	Optional	String	text/plain	Optional - The allowed values are "FIRST_SEEN", "LAST_SEEN" and "UNKNOWN". The default value is "UNKNOWN". This indicates if the <b>timeToLive</b> interval is based on when the data was first seen or last seen.
timeToLive	query	Optional	String	text/plain	Optional - The time to live interval, for example: "1 month" or "5 minutes"
keyNameTypes	query	Optional	Array<Object>	application/json	Optional - A JSON formatted string. This array creates the inner key names and corresponding value types for the table

Table 1352. POST /referencedata/tables response codes

HTTP Response Code	Unique Code	Description
201		A new reference table was successfully created
409	1004	The reference table could not be created, the name provided is already in use. Please change the name and try again.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to create the reference table

## Response Description

Information about the newly created reference table.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
```

```

"key1Label": "String",
"numberOfElements": 0,
"keyNameTypes": {
  "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
}
}

```

## GET /referencedata/tables/{name} DEPRECATED

Return the reference table identified by **name**. If provided, **limit** specifies the number of records to return starting at record specified by **offset**. If not specified, then the first 20 records will be returned.

Table 1353. GET /referencedata/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 1354. GET /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to retrieve
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - The offset value. This indicates to retrieve values starting from the offset value rather than from the beginning of the reference table. The default value is 0.

Table 1355. GET /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has been retrieved
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to retrieve the reference table

## Response Description

The reference table identified by the name specified in the request. The portion of the reference table's data returned is dependent on the limit and offset specified in the request.



## Response Sample

```
{
  "name": "String",
  "elementType": "ALN",
  "createdTime": 1398888888888,
  "timeoutType": "LAST_SEEN",
  "timeToLive": "0 years 1 mons 0 days 0 hours 0 mins 0.00 secs",
  "key1Label": "String",
  "numberOfElements": 6,
  "keyNameTypes": {
    "String1": "ALN",
    "String2": "ALN",
    "String3": "ALN"
  },
  "data": {
    "String2": {
      "String1": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      }
    },
    "String3": {
      "String1": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      },
      "String2": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      }
    },
    "String1": {
      "String1": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      },
      "String2": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      },
      "String3": {
        "value": "String",
        "source": "String",
        "firstSeen": 1398888888888,
        "lastSeen": 1398888888888
      }
    }
  }
}
```

## POST /referencedata/tables/{name} DEPRECATED

Add or update an element in a reference table. The value to be added must be of the appropriate type: either the type that corresponds to the innerKey predefined for the reference table, or the default elementType of the reference table

Table 1356. POST /referencedata/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 1357. POST /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to add or update an element in
outerKey	query	Required	String	text/plain	Required - The outer key for the element to add or update
innerKey	query	Required	String	text/plain	Required - The inner key for the element to add or update
value	query	Required	String	text/plain	Required - The value to add or update in the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.
source	query	Optional	String	text/plain	Optional - An indication of where the data originated. The default value is 'reference data api'

Table 1358. POST /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had an element added or updated
404	1002	The reference table does not exist
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to add or update data in the reference table

## Response Description

Information about the reference table that had an element added or updated. This returns information about the reference table but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
```

```

"timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
"key1Label": "String",
"numberOfElements": 5,
"keyNameTypes": {
  "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
}
}

```

## DELETE /referencedata/tables/{name} DEPRECATED

Remove a reference table or purge its contents

Table 1359. DELETE /referencedata/tables/{name} resource details

<b>MIME Type</b>
application/json

Table 1360. DELETE /referencedata/tables/{name} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove or purge
purgeOnly	query	Optional	String	text/plain	Optional - The allowed values are "false" or "true". The default value is false. This indicates if the reference table should have its contents purged (true), keeping the reference table structure. If the value is "false" or not specified the reference table will be removed completely.

Table 1361. DELETE /referencedata/tables/{name} response codes

HTTP Response Code	Unique Code	Description
200		The reference table has had its contents purged
204		The reference table has been removed
404	1002	The reference table does not exist
409	1004	The reference table could not be deleted, it is being used by other objects.
422	1005	A request parameter is not valid
500	1020	An error occurred while attempting to remove or purge values from the reference table

### Response Description

If the table was removed nothing is returned, otherwise information about the reference table that had its contents purged is returned.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 0,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```

## DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} DEPRECATED

Remove a value from a reference table

Table 1362. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} resource details

MIME Type
application/json

Table 1363. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
name	path	Required	String	text/plain	Required - The name of the reference table to remove a value from
outerKey	path	Required	String	text/plain	Required - The outer key of the value to remove
innerKey	path	Required	String	text/plain	Required - The inner key of the value to remove
value	query	Required	String	text/plain	Required - The value to remove from the reference table. Note: Date values must be represented in milliseconds since the Unix Epoch January 1st 1970.

Table 1364. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} response codes

HTTP Response Code	Unique Code	Description
200		The reference table had had a value removed
404	1002	The reference table does not exist
404	1003	The record does not exist in the reference table
422	1005	A request parameter is not valid

Table 1364. DELETE /referencedata/tables/{name}/{outerKey}/{innerKey} response codes (continued)

HTTP Response Code	Unique Code	Description
500	1020	An error occurred while attempting to remove the reference table value

## Response Description

Information about the reference table that had an element removed. This returns information about table but not the contained data.

## Response Sample

```
{
  "name": "String",
  "elementType": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
  "createdTime": 1397773789254,
  "timeoutType": "String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>",
  "timeToLive": "1 years 1 mons 1 days 1 hours 1 mins 1.11 secs",
  "key1Label": "String",
  "numberOfElements": 5,
  "keyNameTypes": {
    "String3": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String1": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>",
    "String2": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>"
  }
}
```

## Scanner endpoints

Use the references for REST API V4 scanner endpoints.

### GET /scanner/profiles DEPRECATED

Retrieves all of the currently created scan profiles. No parameters are required and the following information should be retrieved for each scan profile - scanProfileId - scanProfileName - description - scanType - scannerName.

Table 1365. GET /scanner/profiles resource details

MIME Type
application/json

There are no parameters for this endpoint.

Table 1366. GET /scanner/profiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

### POST /scanner/profiles/create DEPRECATED

Initiates a request to create a new scanProfile. The request takes one parameter - createScanRequest, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and ips to scan e.g. {'name':'New Scan Profile', 'ips':['10.100.85.135']}

Table 1367. POST /scanner/profiles/create resource details

MIME Type
text/plain

Table 1368. POST /scanner/profiles/create request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 1369. POST /scanner/profiles/create response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
419	9101	Occurs when a parameter is missing or invalid
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been created successfully or not.

## Response Sample

String

### POST /scanner/profiles/start DEPRECATED

Initiates a request to start an already created scanProfile.

The request takes one parameter - scanProfileId. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The scanProfileId will be validated and an appropriate message returned.

Table 1370. POST /scanner/profiles/start resource details

MIME Type
text/plain

Table 1371. POST /scanner/profiles/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
scanProfileId	query	Required	String	text/plain	The unique id of the scan profile we want to start

Table 1372. POST /scanner/profiles/start response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles DEPRECATED

Retrieves all of the currently created scan profiles. No parameters are required and the following information should be retrieved for each scan profile - scanProfileId - name - description - scanType - scannerName - schedule - status - progress - endTime - duration

Table 1373. GET /scanner/scanprofiles resource details

MIME Type
application/json

Table 1374. GET /scanner/scanprofiles request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.

Table 1374. GET /scanner/scanprofiles request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 1375. GET /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The list of scan profiles was successfully returned
500	1030	Occurs when an attempt is made to list scan profiles when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
      "hours": 42,
      "minutes": 42,
      "month": 42,
      "seconds": 42,
      "time": 42,
      "timezoneOffset": 42,
      "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
  }
]
```



## POST /scanner/scanprofiles DEPRECATED

Initiates a request to create a new scanProfile. The request takes one parameter - createScanRequest, which is just a POJO. To create the scan, you will need to build up a JSON object that contains the Scan Profile name and hosts to scan e.g. {'name':'New Scan Profile', 'hosts':['10.100.85.135']}

Table 1376. POST /scanner/scanprofiles resource details

MIME Type
text/plain

Table 1377. POST /scanner/scanprofiles request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	Object	application/json	null	{ "description": "String", "hosts": [ "String" ], "name": "String" }

Table 1378. POST /scanner/scanprofiles response codes

HTTP Response Code	Unique Code	Description
200		The scan has been successfully created
500	1030	Occurs when an attempt is made to create a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been created successfully or not.

## Response Sample

String

## GET /scanner/scanprofiles/{profileid} DEPRECATED

Retrieves a scan profile for a given Scan Profile ID. The only parameter required is the Scan Profile ID. The following information about a scan profile will be returned - scanProfileId - name - description - scanType - scannerName - schedule - status - progress - endTime - duration

Table 1379. GET /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 1380. GET /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we need to retrieve information for

Table 1380. GET /scanner/scanprofiles/{profileid} request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.
filter	query	Optional	String	text/plain	Optional - This parameter is used to restrict the elements in a list base on the contents of various fields.
Range	header	Optional	String	text/plain	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

Table 1381. GET /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
200		The scan profile was successfully returned
500	1030	Occurs when an attempt is made to list a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

The list of scan profiles currently configured in QVM

## Response Sample

```
[
  {
    "description": "String",
    "duration": {
      "days": 42,
      "hours": 42,
      "minutes": 42,
      "months": 42,
      "seconds": 42.5,
      "type": "String",
      "value": "String",
      "years": 42
    },
    "endTime": {
      "date": 42,
      "day": 42,
```

```

        "hours": 42,
        "minutes": 42,
        "month": 42,
        "seconds": 42,
        "time": 42,
        "timezoneOffset": 42,
        "year": 42
    },
    "progress": 42,
    "scanProfileId": 42,
    "scanProfileName": "String",
    "scanType": "String",
    "scannerName": "String",
    "schedule": "String",
    "status": "String"
}
]

```

## POST /scanner/scanprofiles/{profileid} DEPRECATED

Update a scan profile. The Scan Profile ID is required. The following information on a scan profile can be updated - name - description - ips eg {'name': 'Updated Scan Profile', 'ips': ['10.100.85.135']}

Table 1382. POST /scanner/scanprofiles/{profileid} resource details

MIME Type
application/json

Table 1383. POST /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile used to update

Table 1384. POST /scanner/scanprofiles/{profileid} request body details

Parameter	Data Type	MIME Type	Description	Sample
scanProfile	JSON	application/json	null	null

Table 1385. POST /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
202		The scan profile was successfully updated
500	1030	Occurs when an attempt is made to update a scan profile when certain conditions are not met, or when too many scan requests have been made

## Response Description

A message to indicate whether the scan profile has updated or not.

## Response Sample

### DELETE /scanner/scanprofiles/{profileid} DEPRECATED

Initiates a request to delete a scanProfile. The request takes one parameter - the Scan Profile ID.

Table 1386. DELETE /scanner/scanprofiles/{profileid} resource details

MIME Type
text/plain

Table 1387. DELETE /scanner/scanprofiles/{profileid} request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	null

Table 1388. DELETE /scanner/scanprofiles/{profileid} response codes

HTTP Response Code	Unique Code	Description
204		The scan has been successfully deleted
500	1030	Occurs when an attempt is made to delete a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been deleted successfully or not.

## Response Sample

String

### POST /scanner/scanprofiles/{profileid}/start DEPRECATED

Initiates a request to start an already created scanProfile.

The request takes one parameter - scanProfileId, and one optional parameter - ips. To get a list of scanProfileIds, simply get a list of the current scan profiles by initiating a 'profiles' request on the scanner endpoint. The scanProfileId will be validated and an appropriate message returned.

Table 1389. POST /scanner/scanprofiles/{profileid}/start resource details

MIME Type
text/plain

Table 1390. POST /scanner/scanprofiles/{profileid}/start request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
profileid	path	Required	String	text/plain	The unique id of the scan profile we want to start

Table 1391. POST /scanner/scanprofiles/{profileid}/start request body details

Parameter	Data Type	MIME Type	Description	Sample
ips	JSON	application/json	null	null

Table 1392. POST /scanner/scanprofiles/{profileid}/start response codes

HTTP Response Code	Unique Code	Description
202		The scan has been successfully started
403	1000	Occurs if the user does not have permission to start a scan, or the scan is in progress
500	1030	Occurs when an attempt is made to start a scan when certain conditions are not met, or when too many scan requests have been made

## Response Description

An indicator of whether the scan has been started successfully or not.

## Response Sample

String

## Offense endpoints

Use the references for REST API V2 Offense endpoints.

### GET /siem/offenses DEPRECATED

Retrieve a list of offenses currently in the system.

Retrieve a list of offenses currently in the system.

Table 1393. GET /siem/offenses resource details

MIME Type
application/json

Table 1394. GET /siem/offenses request parameter details

Parameter	Type	Optionality	Data Type	MIME Type	Description
limit	query	Optional	Number (Integer)	text/plain	Optional - The number of records to return. The default value is 20.
offset	query	Optional	Number (Integer)	text/plain	Optional - This parameter indicates to retrieve offenses that start from the offset value rather than from the beginning of the offenses. The default value is 0.

Table 1394. GET /siem/offenses request parameter details (continued)

Parameter	Type	Optionality	Data Type	MIME Type	Description
fields	query	Optional	String	text/plain	Optional - Use this parameter to specify which fields you would like to get back in the response. Fields that are not named are excluded. Specify subfields in brackets and multiple fields in the same object are separated by commas.

Table 1395. GET /siem/offenses response codes

HTTP Response Code	Unique Code	Description
200		The offense list was retrieved.
422	1005	A request parameter is not valid.
500	1020	An error occurred while the offense list was being retrieved.

## Response Description

An array of offense objects. An offense object contains the following fields:

- **id** - Number - The ID of the offense.
- **description** - String - The description of the offense.
- **assigned\_to** - String - The user the offense is assigned to.
- **categories** - Array of strings - Event categories that are associated with the offense.
- **category\_count** - Number - The number of event categories that are associated with the offense.
- **policy\_category\_count** - Number - The number of policy event categories that are associated with the offense.
- **security\_category\_count** - Number - The number of security event categories that are associated with the offense.
- **close\_time** - Number - The number of milliseconds since epoch when the offense was closed.
- **close\_user** - String - The user that closed the offense.
- **closing\_reason** - String - The reason the offense was closed.
- **credibility** - Number - The credibility of the offense.
- **relevance** - Number - The relevance of the offense.
- **severity** - Number - The severity of the offense.
- **magnitude** - Number - The magnitude of the offense.
- **destination\_networks** - Array of strings - The destination networks that are associated with the offense.
- **source\_network** - String - The source network that is associated with the offense.

- **device\_count** - Number - The number of devices that are associated with the offense.
- **event\_count** - Number - The number of events that are associated with the offense.
- **flow\_count** - Number - The number of flows that are associated with the offense.
- **inactive** - Boolean - True if the offense is inactive.
- **last\_updated\_time** - Number - The number of milliseconds since epoch when the offense was last updated.
- **local\_destination\_count** - Number - The number of local destinations that are associated with the offense.
- **offense\_source** - String - The source of the offense.
- **offense\_type** - Number - A number that represents the offense type. See the Offense Type Codes table for the code to offense type mapping.
- **protected** - Boolean - True if the offense is protected.
- **remote\_destination\_count** - Number - The number of remote destinations that are associated with the offense.
- **source\_count** - Number - The number of sources that are associated with the offense.
- **start\_time** - Number - The number of milliseconds since epoch when the offense was started.
- **status** - String - The status of the offense. One of "OPEN", "HIDDEN", or "CLOSED".
- **username\_count** - The number of usernames that are associated with the offense.

Table 1396. Offense Type Codes

Code	Offense Type
Code	Offense Type
0	Source IP
1	Destination IP
2	Event Name
3	Username
4	Source MAC Address
5	Destination MAC Address
6	Log Source
7	Hostname
8	Source Port
9	Destination Port
10	Source IPv6
11	Destination IPv6
12	Source ASN
13	Destination ASN
14	Rule
15	App Id
18	Scheduled Search

## Response Sample

```
[{"credibility": 42,
  "close_user": "String",
  "remote_destination_count": 42,
  "assigned_to": "String",
  "local_destination_count": 42,
  "source_count": 42,
  "closing_reason": "String",
  "start_time": 42,
  "id": 42,
  "destination_networks": ["String"],
  "inactive": true,
  "protected": true,
  "policy_category_count": 42,
  "description": "String",
  "category_count": 42,
  "relevance": 42,
  "device_count": 42,
  "security_category_count": 42,
  "flow_count": 42,
  "event_count": 42,
  "offense_source": "String",
  "status": "String",
  "magnitude": 42,
  "severity": 42,
  "username_count": 42,
  "close_time": 42,
  "source_network": "String",
  "last_updated_time": 42,
  "categories": ["String"],
  "offense_type": 42}]
```



---

## Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
170 Tracer Lane,  
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable

information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.







Printed in USA