
Micro Focus Security ArcSight Intelligence SaaS

Software Version: 6.4.5

Developer's Guide

Document Release Date: April 2023

Software Release Date: April 2023



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2023 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Introduction	34
Intended Audience	34
Construct API URLs	34
Retrieve Paginated API Responses	34
Render Anomalies	35
Use the API with the Swagger UI	36
Example: Call an Endpoint	37
Tuning API Reference	37
Alert Templates	37
post <code>/{tid}/alert_templates</code>	37
Consumes	37
Produces	37
Path parameters	38
Request body	38
Responses	38
get <code>/{tid}/alert_templates/{anomalyType}/{did}</code>	38
Produces	38
Path parameters	38
Return type	38
Example data	38
Responses	39
Anomaly Meta	39
post <code>/{tid}/anomaly_meta</code>	39
Consumes	39
Produces	40
Path parameters	40
Request body	40
Responses	40
delete <code>/{tid}/anomaly_meta/{anomalyType}</code>	40
Produces	40
Path parameters	40
Responses	40
get <code>/{tid}/anomaly_meta/{anomalyType}</code>	41
Produces	41
Path parameters	41
Return type	41

Example data	41
Responses	41
get /{tid}/anomaly_meta	41
Produces	41
Path parameters	42
Return type	42
Example data	42
Responses	42
put /{tid}/anomaly_meta/{anomalyType}	42
Consumes	42
Produces	42
Path parameters	43
Request body	43
Responses	43
delete /{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}	43
Produces	43
Path parameters	43
Responses	44
get /{tid}/did_tags	44
Produces	44
Path parameters	44
Return type	44
Example data	44
Responses	45
get /{tid}/did_tags/{ds}	45
Produces	45
Path parameters	45
Return type	45
Example data	45
Responses	46
get /{tid}/did_tags/{ds}/{did}	46
Produces	46
Path parameters	46
Return type	46
Example data	46
Responses	47
get /{tid}/did_tags/{ds}/{did}/{type}	47
Produces	47
Path parameters	47

Return type	47
Example data	47
Responses	48
get /{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}	48
Produces	48
Path parameters	48
Return type	49
Example data	49
Responses	49
get /{tid}/did_tags/{ds}/{did}/{type}/{identifier}	49
Produces	49
Path parameters	49
Return type	50
Example data	50
Responses	50
put /{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}	50
Consumes	50
Produces	51
Path parameters	51
Request body	51
Responses	51
Entity Mappings	51
post /{tid}/entity_mappings	51
Consumes	51
Produces	52
Path parameters	52
Request body	52
Responses	52
delete /{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}	52
Produces	52
Path parameters	52
Responses	53
get /{tid}/entity_mappings/{ds}/{did}/{entityType}	53
Produces	53
Path parameters	53
Return type	53
Example data	53
Responses	54
get /{tid}/entity_mappings/{ds}/{did}	54

Produces	54
Path parameters	54
Return type	54
Example data	54
Responses	55
get /{tid}/entity_mappings/{ds}	55
Produces	55
Path parameters	55
Return type	55
Example data	55
Responses	56
get /{tid}/entity_mappings	56
Produces	56
Path parameters	56
Return type	56
Example data	56
Responses	57
get /{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}	57
Produces	57
Path parameters	57
Return type	58
Example data	58
Responses	58
put /{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}	58
Consumes	58
Produces	58
Path parameters	58
Request body	59
Responses	59
Entity Tags	59
post /{tid}/entity_tags	59
Consumes	59
Produces	59
Path parameters	59
Request body	59
Responses	60
delete /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}	60
Produces	60
Path parameters	60

Responses	60
get /{tid}/entity_tags	60
Produces	61
Path parameters	61
Return type	61
Example data	61
Responses	61
get /{tid}/entity_tags/{ds}	61
Produces	62
Path parameters	62
Return type	62
Example data	62
Responses	62
get /{tid}/entity_tags/{ds}/{did}	62
Produces	63
Path parameters	63
Return type	63
Example data	63
Responses	63
get /{tid}/entity_tags/{ds}/{did}/{type}	64
Produces	64
Path parameters	64
Return type	64
Example data	64
Responses	65
get /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}	65
Produces	65
Path parameters	65
Return type	65
Example data	65
Responses	66
get /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}	66
Produces	66
Path parameters	66
Return type	66
Example data	66
Responses	67
put /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}	67
Consumes	67

Produces	67
Path parameters	67
Request body	68
Responses	68
Example Anomalies	68
get <code>/{tid}/alert_templates/example/{anomaly_type}</code>	68
Produces	68
Path parameters	68
Return type	68
Example data	69
Responses	69
post <code>/{tid}/importance</code>	69
Consumes	69
Produces	69
Path parameters	70
Request body	70
Responses	70
delete <code>/{tid}/importance/{entityType}/{entityId}</code>	70
Produces	70
Path parameters	70
Responses	70
get <code>/{tid}/importance/{entityType}/{entityId}</code>	70
Produces	71
Path parameters	71
Return type	71
Example data	71
Responses	71
get <code>/{tid}/importance</code>	71
Produces	71
Path parameters	72
Return type	72
Example data	72
Responses	72
get <code>/{tid}/importance/{entityType}</code>	72
Produces	72
Path parameters	73
Return type	73
Example data	73
Responses	73

put <code>/{tid}/importance/{entityType}/{entityId}</code>	73
Consumes	73
Produces	74
Path parameters	74
Request body	74
Responses	74
Parameters	74
post <code>/{tid}/parameters</code>	74
Consumes	74
Produces	74
Path parameters	75
Request body	75
Responses	75
delete <code>/{tid}/parameters/{name}</code>	75
Produces	75
Path parameters	75
Responses	75
get <code>/{tid}/parameters/{name}</code>	75
Produces	76
Path parameters	76
Return type	76
Example data	76
Responses	76
get <code>/{tid}/parameters</code>	76
Produces	76
Path parameters	77
Return type	77
Example data	77
Responses	77
put <code>/{tid}/parameters/{name}</code>	77
Consumes	77
Produces	77
Path parameters	78
Request body	78
Responses	78
Relation Tags	78
post <code>/{tid}/relation_tags</code>	78
Consumes	78
Produces	78

Path parameters	78
Request body	78
Responses	79
delete /{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}	79
Produces	79
Path parameters	79
Responses	79
get /{tid}/relation_tags	79
Produces	80
Path parameters	80
Return type	80
Example data	80
Responses	80
get /{tid}/relation_tags/{ds}	80
Produces	81
Path parameters	81
Return type	81
Example data	81
Responses	81
get /{tid}/relation_tags/{ds}/{did}	81
Produces	82
Path parameters	82
Return type	82
Example data	82
Responses	82
get /{tid}/relation_tags/{ds}/{did}/{type}	83
Produces	83
Path parameters	83
Return type	83
Example data	83
Responses	84
get /{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}	84
Produces	84
Path parameters	84
Return type	84
Example data	84
Responses	85
get /{tid}/relation_tags/{ds}/{did}/{type}/{identifier}	85
Produces	85

Path parameters	85
Return type	85
Example data	85
Responses	86
put <code>/{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}</code>	86
Consumes	86
Produces	86
Path parameters	86
Request body	87
Responses	87
Violations	87
get <code>/{tid}/violations/{violationName}</code>	87
Produces	87
Path parameters	87
Return type	87
Example data	88
Responses	88
get <code>/{tid}/violations</code>	88
Produces	88
Path parameters	88
Return type	88
Example data	89
Responses	89
post <code>/{tid}/violations/register</code>	89
Consumes	89
Produces	89
Path parameters	90
Request body	90
Responses	90
Weights	90
post <code>/{tid}/weights</code>	90
Consumes	90
Produces	90
Path parameters	90
Request body	90
Responses	91
delete <code>/{tid}/weights/{did}/{anomalyType}</code>	91
Produces	91
Path parameters	91

Responses	91
get /{tid}/weights/{did}/{anomalyType}	91
Produces	91
Path parameters	92
Return type	92
Example data	92
Responses	92
get /{tid}/weights	92
Produces	92
Path parameters	93
Return type	93
Example data	93
Responses	93
get /{tid}/weights/{did}	93
Produces	93
Path parameters	94
Return type	94
Example data	94
Responses	94
put /{tid}/weights/{did}/{anomalyType}	94
Consumes	95
Produces	95
Path parameters	95
Request body	95
Responses	95
Models	95
AlertTemplate	95
AlertsMeta	96
AlertsMetaSimple	97
AlertsMetaViolations	97
AnomalyMeta	97
EntityMapping	98
EntityTag	98
ExampleAnomaly	99
Importance	100
Parameter	100
RelationTag	100
Weight	101
Analytics API Reference	101

actions	101
post /actions/login	101
Consumes	101
Produces	102
Request body	102
Return type	102
Example data	102
Responses	102
get /actions/logoff	102
Consumes	102
Produces	102
Request headers	103
Return type	103
Example data	103
Responses	103
get /actions/logoff/saml	103
Consumes	103
Produces	103
Request headers	104
Query parameters	104
Responses	104
get /actions/login/oauth2	104
Consumes	104
Produces	104
Query parameters	104
Responses	104
get /actions/login/oauth2/callback	104
Consumes	105
Produces	105
Query parameters	105
Responses	105
get /actions/logoff/oauth2	105
Consumes	105
Produces	105
Request headers	105
Query parameters	106
Responses	106
get /actions/login/oauth2/renew	106
Consumes	106

Produces	106
Request headers	106
Responses	106
get /actions/login/saml	106
Example Response (Status 200)	107
Consumes	107
Produces	107
Query parameters	107
Responses	107
post /actions/login/saml/sso	107
Consumes	108
Produces	108
Form parameters	108
Responses	108
dashboards{tenantId}	108
post /dashboards/{tid}	108
Example Request Body	108
Consumes	108
Produces	109
Path parameters	109
Request body	109
Return type	109
Example data	109
Responses	109
put /dashboards/{tid}/tags/{id}	110
Example Request Body	110
Produces	110
Path parameters	110
Request body	110
Responses	110
delete /dashboards/{tid}/tags/{id}	110
Produces	111
Path parameters	111
Responses	111
get /dashboards/{tid}/{id}	111
Example Response (Status 200)	111
Produces	111
Path parameters	112
Return type	112

Example data	112
Responses	112
get /dashboards/{tid}	112
Example Response (Status 200)	113
Produces	113
Path parameters	114
Return type	114
Example data	114
Responses	115
get /dashboards/{tid}/home	115
Example Response (Status 200)	115
Produces	115
Path parameters	115
Responses	116
get /dashboards/{tid}/tags	116
Example Request Body	116
Produces	116
Path parameters	116
Return type	116
Example data	116
Responses	117
delete /dashboards/{tid}/{id}	117
Produces	117
Path parameters	117
Responses	117
delete /dashboards/{tid}/home	117
Produces	118
Path parameters	118
Responses	118
put /dashboards/{tid}/home/{id}	118
Produces	118
Path parameters	118
Responses	118
put /dashboards/{tid}/{id}	118
Example Request Body	119
Consumes	119
Produces	119
Path parameters	119
Request body	119

Return type	119
Example data	119
Responses	120
events{tenantId}	120
post /events/{tid}/savedSearches	120
Consumes	120
Produces	120
Path parameters	120
Request body	121
Return type	121
Example data	121
Responses	123
get /events/{tid}/savedSearches	123
Produces	123
Path parameters	123
Return type	123
Example data	124
Responses	128
delete /events/{tid}/savedSearches/{id}	128
Produces	128
Path parameters	128
Responses	128
delete /events/{tid}/savedSearches/{id}/draft	129
Produces	129
Path parameters	129
Responses	129
put /events/{tid}/savedSearches/{id}	129
Consumes	129
Produces	129
Path parameters	129
Request body	130
Return type	130
Example data	130
Responses	132
put /events/{tid}/savedSearches/{id}/draft	132
Consumes	132
Produces	132
Path parameters	133
Request body	133

Return type	133
Example data	133
Responses	134
info	134
get /info/auth	134
Example Response (Status 200)	134
Produces	135
Responses	135
get /info/analysedEntities/{tid}	135
Example Response (Status 200)	135
Filtering the results	135
Produces	135
Path parameters	135
Query parameters	135
Responses	136
get /info/deployment	136
Example Response (Status 200)	136
Produces	136
Responses	136
get /info/session	136
Produces	136
Return type	136
Example data	137
Responses	138
get /info/build	138
Example Response (Status 200)	138
Produces	138
Responses	138
rawEvents{tenantId}	138
post /rawEvents/{tid}/typeAhead	139
Produces	139
Path parameters	139
Request body	139
Request headers	139
Query parameters	139
Responses	139
get /rawEvents/{tid}/csv	140
Produces	140
Path parameters	140

Query parameters	140
Responses	140
get /rawEvents/{tid}	141
Produces	141
Path parameters	141
Request headers	141
Query parameters	141
Responses	142
post /rawEvents/{tid}/graph	142
Consumes	142
Produces	142
Path parameters	142
Request body	142
Request headers	142
Query parameters	143
Responses	143
post /rawEvents/{tid}/resolve	143
Consumes	143
Produces	143
Path parameters	143
Request body	143
Request headers	144
Query parameters	144
Responses	144
get /rawEvents/{tid}/resolve/{id}	144
Consumes	144
Produces	144
Path parameters	145
Request headers	145
Query parameters	145
Responses	145
post /rawEvents/{tid}/search	145
Consumes	146
Produces	146
Path parameters	146
Request body	146
Request headers	146
Query parameters	146
Responses	147

search{tenantId}	147
get /search/{tid}/{rollupLevel}/breakdown/risk	147
Example Response (Status 200)	147
Filtering the results	147
Produces	148
Path parameters	148
Request headers	148
Query parameters	148
Responses	149
get /search/{tid}/{rollupLevel}	149
Example Response (Status 200)	149
Filtering the results	150
Produces	151
Path parameters	151
Request headers	151
Query parameters	151
Responses	152
get /search/{tid}/{rollupLevel}/count	152
Example Response (Status 200)	152
Filtering the results	153
Produces	153
Path parameters	153
Request headers	153
Query parameters	154
Responses	154
get /search/{tid}/{rollupLevel}/{rollupId}	154
Example Response (Status 200)	155
Filtering the results	156
Produces	156
Path parameters	156
Request headers	156
Query parameters	157
Responses	157
get /search/{tid}/controllers/authentications	157
Example Response (Status 200)	157
Filtering the results	157
Produces	158
Path parameters	158
Request headers	158

Query parameters	158
Responses	158
get /search/{tid}/{rollupLevel}/{rollupId}/context	159
Example Response (Status 200)	159
Filtering the results	159
Produces	160
Path parameters	160
Request headers	160
Responses	160
get /search/{tid}/{entityType}	160
Example Response (Status 200)	160
Produces	161
Path parameters	161
Request headers	161
Query parameters	161
Responses	162
get /search/{tid}/{entityType}/{entityHash}	162
Produces	162
Path parameters	162
Request headers	163
Responses	163
post /search/{tid}/entityByName	163
Produces	163
Path parameters	163
Request body	164
Request headers	164
Responses	164
get /search/{tid}/{entityType}/{entityHash}/risk	164
Example Response (Status 200)	164
Produces	165
Path parameters	165
Request headers	166
Query parameters	166
Responses	166
get /search/{tid}/{entityType}/{entityHash}/riskGraph	167
Example Response (Status 200)	167
Produces	167
Path parameters	167
Request headers	168

Query parameters	168
Responses	168
get /search/{tid}/users/bots	168
Example Response (Status 200)	169
Produces	169
Path parameters	169
Request headers	169
Query parameters	170
Responses	170
get /search/{tid}/distribution/risk	170
Example Response (Status 200)	170
Filtering the results	170
Produces	171
Path parameters	171
Request headers	171
Query parameters	171
Responses	172
get /search/{tid}/{entityType}/distribution/risk	172
Example Response (Status 200)	172
Filtering the results	172
Produces	173
Path parameters	173
Request headers	173
Query parameters	173
Responses	173
get /search/{tid}/info	174
Example Response (Status 200)	174
Produces	176
Path parameters	176
Request headers	176
Query parameters	176
Responses	177
get /search/{tid}/matrix/{type}	177
Example Response (Status 200)	177
Filtering the results	180
Produces	180
Path parameters	180
Request headers	181
Query parameters	181

Responses	181
get /search/{tid}/riskGraph/breakdown	181
Example Response (Status 200)	182
Filtering the results	183
Produces	183
Path parameters	183
Request headers	183
Query parameters	183
Responses	184
get /search/{tid}/riskGraph	184
Example Response (Status 200)	185
Filtering the results	185
Produces	185
Path parameters	186
Request headers	186
Query parameters	186
Responses	186
get /search/{tid}/riskyHours	187
Example Response (Status 200)	187
Filtering the results	187
Produces	188
Path parameters	188
Request headers	188
Query parameters	188
Responses	189
get /search/{tid}/templates	189
Example Response (Status 200)	189
Produces	190
Path parameters	190
Request headers	190
Query parameters	190
Responses	190
get /search/{tid}/{entityType}/topAccessed	190
Example Response (Status 200)	191
Filtering the results	191
Produces	192
Path parameters	192
Request headers	192
Query parameters	192

Responses	193
get /search/{tid}/users/topExitProducers	193
Example Response (Status 200)	193
Filtering the results	194
Produces	194
Path parameters	194
Request headers	194
Query parameters	194
Responses	195
get /search/{tid}/users/topFailedLogin	195
Example Response (Status 200)	195
Filtering the results	196
Produces	196
Path parameters	196
Request headers	196
Query parameters	196
Responses	197
get /search/{tid}/users/topScreenCaptures	197
Example Response (Status 200)	197
Filtering the results	198
Produces	198
Path parameters	198
Request headers	198
Query parameters	199
Responses	199
get /search/{tid}/users/topViolationProducers	199
Example Response (Status 200)	199
Filtering the results	200
Produces	200
Path parameters	201
Request headers	201
Query parameters	201
Responses	201
get /search/{tid}/typeAhead	201
Example Response (Status 200)	202
Produces	202
Path parameters	202
Request headers	203
Query parameters	203

Responses	203
get /search/{tid}/users/{userHash}/workingHours/daily	203
Example Response (Status 200)	204
Produces	204
Path parameters	204
Request headers	204
Responses	205
get /search/{tid}/users/workingHours/weekly	205
Example Response (Status 200)	205
Produces	206
Path parameters	206
Request headers	206
Responses	206
get /search/{tid}/users/workingHours/daily	206
Example Response (Status 200)	206
Produces	207
Path parameters	207
Request headers	207
Responses	207
get /search/{tid}/users/{userHash}/workingHours/weekly	207
Example Response (Status 200)	208
Produces	208
Path parameters	208
Request headers	209
Responses	209
get /search/{tid}/topRisky	209
Example Response (Status 200)	209
Filtering the results	210
Produces	210
Path parameters	210
Request headers	210
Query parameters	210
Responses	211
get /search/{tid}/{entityType}/topRisky	211
Example Response (Status 200)	212
Filtering the results	212
Produces	213
Path parameters	213
Request headers	213

Query parameters	213
Responses	214
get /search/{tid}/{rollupLevel}/{rollupId}/expand	214
Example Response (Status 200)	214
Filtering the results	215
Produces	215
Path parameters	216
Request headers	216
Query parameters	216
Responses	217
search{tenantId}meta	217
post /search/{tid}/meta	217
Example Response (Status 200)	217
Consumes	218
Produces	218
Path parameters	218
Request body	218
Request headers	218
Responses	218
delete /search/{tid}/meta/{metaId}	218
Example Response (Status 200)	219
Consumes	219
Produces	219
Path parameters	219
Request headers	219
Responses	219
get /search/{tid}/meta/log	219
Example Response (Status 200)	220
Consumes	220
Produces	221
Path parameters	221
Request headers	221
Query parameters	221
Responses	222
get /search/{tid}/meta/{metaId}	222
Example Response (Status 200)	222
Consumes	223
Produces	223
Path parameters	223

Request headers	223
Responses	223
get /search/{tid}/meta	223
Example Response (Status 200)	223
Consumes	224
Produces	224
Path parameters	224
Request headers	225
Query parameters	225
Responses	225
put /search/{tid}/meta/{metaId}	226
Example Response (Status 200)	226
Consumes	226
Produces	226
Path parameters	226
Request body	227
Request headers	227
Responses	227
search{tenantId}tags	227
put /search/{tid}/tags/{tagId}/{tagElementType}/{elementHash}	227
Example Response (Status 200)	227
Consumes	227
Produces	228
Path parameters	228
Request headers	228
Query parameters	228
Responses	228
post /search/{tid}/tags/{tagId}/{tagElementType}/add	228
Example Response (Status 200)	229
Consumes	229
Produces	229
Path parameters	229
Request body	229
Request headers	229
Query parameters	230
Responses	230
post /search/{tid}/tags	230
Example Response (Status 200)	230
Consumes	230

Produces	230
Path parameters	231
Request body	231
Request headers	231
Responses	231
delete /search/{tid}/tags/{tagId}	231
Example Response (Status 200)	231
Consumes	231
Produces	232
Path parameters	232
Request headers	232
Query parameters	232
Responses	232
get /search/{tid}/tags/{tagId}/{tagElementType}	232
Example Response (Status 200)	232
Consumes	233
Produces	233
Path parameters	233
Request headers	233
Query parameters	233
Responses	233
get /search/{tid}/tags/{tagId}	234
Example Response (Status 200)	234
Consumes	234
Produces	234
Path parameters	234
Request headers	234
Responses	235
get /search/{tid}/tags/{boolOperator}/entities	235
Example Response (Status 200)	235
Consumes	235
Produces	235
Path parameters	235
Request headers	236
Query parameters	236
Responses	236
get /search/{tid}/tags	236
Example Response (Status 200)	236
Filtering the results	237

Consumes	237
Produces	237
Path parameters	237
Request headers	238
Query parameters	238
Responses	238
delete /search/{tid}/tags/{tagId}/{tagElementType}/{elementHash}	238
Example Response (Status 200)	238
Consumes	239
Produces	239
Path parameters	239
Request headers	239
Query parameters	239
Responses	239
post /search/{tid}/tags/{tagId}/{tagElementType}/remove	239
Example Response (Status 200)	240
Consumes	240
Produces	240
Path parameters	240
Request body	240
Request headers	240
Query parameters	241
Responses	241
post /search/{tid}/tags/{tagId}/update	241
Example Response (Status 200)	241
Consumes	241
Produces	241
Path parameters	242
Request body	242
Request headers	242
Responses	242
tenants	242
delete /tenants/{tid}	242
Produces	242
Path parameters	242
Responses	243
delete /tenants/{tid}/users/{userId}	243
Produces	243
Path parameters	243

Responses	243
get /tenants/{tid}	243
Produces	243
Path parameters	243
Return type	244
Example data	244
Responses	244
get /tenants/{tid}/users	244
Produces	244
Path parameters	244
Return type	244
Example data	244
Responses	245
get /tenants	245
Produces	245
Return type	245
Example data	246
Responses	246
get /tenants/{tid}/users/{userId}	246
Produces	246
Path parameters	246
Return type	246
Example data	246
Responses	247
put /tenants/{tid}	247
Consumes	247
Produces	247
Path parameters	247
Request body	247
Return type	247
Example data	248
Responses	248
put /tenants	248
Consumes	248
Request body	248
Responses	248
put /tenants/{tid}/users/{userId}	248
Consumes	249
Produces	249

Path parameters	249
Request body	249
Request headers	249
Return type	249
Example data	249
Responses	250
theme	250
delete /theme/{tid}	250
Produces	250
Path parameters	250
Responses	250
delete /theme	250
Produces	250
Responses	251
get /theme	251
Example Response (Status 200)	251
Produces	251
Responses	251
get /theme/{tid}	251
Example Response (Status 200)	252
Produces	252
Path parameters	252
Responses	252
put /theme	252
Example Request Body	253
Consumes	253
Produces	253
Request body	253
Responses	253
put /theme/{tid}	253
Example Request Body	254
Consumes	254
Produces	254
Path parameters	254
Request body	254
Responses	254
url	254
post /url	255
Example Request Body	255

Example Response (Status 200)	255
Produces	255
Request body	255
Return type	255
Example data	255
Responses	255
get /url/{hash}	256
Produces	256
Path parameters	256
Responses	256
users	256
get /users	256
Produces	256
Return type	256
Example data	256
Responses	257
Models	257
ApiAction	257
ApiCredentials	257
ApiDashboard	257
ApiDashboardTag	258
ApiEntityNameRequest	258
ApiHash	258
ApiMetaRequest	258
ApiSavedSearches	259
ApiSavedSearchesDraft	260
ApiSavedSearchesResponse	260
ApiSessionTenant	260
ApiSimpleDashboard	261
ApiSimpleDashboardTag	261
ApiTagEntities	261
ApiTenantUser	261
ApiTheme	262
ApiUrl	263
DbUser	263
JsonNode	263
LoginResponse	265
RawEventsGraphRequest	265
RawEventsRequest	265

RawEventsTypeaheadRequest	266
ServiceProxyInfo	266
Session	267
SessionInfo	267
SortField	268
TagBase	268
Tenant	268
Exports API Reference	269
Construct Exports API URLs	269
Exports API Endpoints	269
GET /dashboard	269
Consumes	269
Produces	269
Query Parameters	269
Return type	270
Responses	270
GET /info/build	270
Example Response (Status 200)	270
Produces	270
Responses	270
Send Documentation Feedback	271

Introduction

This guide describes how to use the Intelligence REST API, which allows you to manage, develop, and interface with analytics data. This API also provides access to analytics results and related tuning parameters.

Intended Audience

This Guide assumes that you are an experienced programmer and are familiar with REST APIs, web programming, and your organization's server environment, security infrastructure, and data sources.

You should also be familiar with the business needs of your organization.

Construct API URLs

To call an endpoint in this API, use the fully-qualified domain name (FQDN) of ArcSight SaaS Intelligence, and append the base path (`/interset/api`) followed by the path listed in the [Tuning API Reference](#) and [Analytics API Reference](#). For example, to call the `GET /tenants` endpoint, use the following URL with the `GET` method:

```
https://<FQDN of Intelligence>/interset/api/tenants
```

Retrieve Paginated API Responses

Some endpoints return paginated results. These endpoints include a field called `scrollId` in their responses. To retrieve the next page of results from the same call, call the endpoint again with the same parameters, but this time pass the `scrollId` from the current response in the `scrollId` query parameter of the new API call.

For example, the response from the `GET /search/{tid}/{entityType}/topRisky` endpoint looks similar to the following:

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "bc23443bd21342fa8997e",
      "entityType": "user",
      "entityName": "Annie",
      "risk": 25,
    }
  ]
}
```

```

    "riskChange": 0,
    "storyCount": 3,
    "lastActivity": 1453957200,
    "preDecayedRisk": 0,
    "decayedToTimestamp": 0,
    "mostSignificantAlert": null,
    "tags": [
      {
        "id": "9v3sdqdC2jd0FJCBuYcAPw",
        "name": "reviewed",
        "source": "user",
        "description": ""
      }
    ]
  },
],
"totalHits": 25,
"scrollId": "vabsjk5h24elkdasjfojdabhgjk32b5b",
"cached": false
}

```

Note the returned `scrollId`. To get the next set of results, call the GET `/search/{tid}/{entityType}/topRisky` endpoint again, but pass the `scrollId` as a query parameter:

```

curl -X GET --header 'Accept: text/plain' \
  'https://<reporting_fqdn>/interaset/api/search/<tenant_ID>/files/topRisky?scrollid=vabsjk5h24elkdasjfojdabhgjk32b5b'

```

Render Anomalies

For some of the search endpoints, you can specify a `markup` parameter. When `markup` is `false`, the returned anomalies contain only English text that can be directly displayed without further processing. When `markup` is `true`, the anomalies may contain markup tags in double curly braces, `{{` and `}}`. The possible tags are as follows:

- **timestamp**

The anomaly time.

The timestamp corresponds to the start of the hour in which the anomaly occurs. For example:

```
"...{{timestamp ms=\"1516748280000\" joda=\"h\" moment=\"h\"}} ..."
```

The **timestamp** can include the following fields:

- **ms**: the epoch (Unix) timestamp. Epoch timestamps are expressed in GMT (i.e., they don't contain time zone information). Usually this timestamp would be rendered in the

browser's time zone.

- **joda**: specifies the format to use when rendering with Joda-Time.
- **moment**: specifies the format to use when rendering with Moment.js or date-fns.

If the **moment** field isn't present, the Intelligence UI uses the format string "dddd".

- **entity**

The entity that the text pertains to. For example:

```
"... {{entity name=\"katherine.white\" hash=\"28044feb24be66c7\"
type=\"user\" risk=21 showRiskBall=false}} ..."
```

The **entity** can include the following fields:

- **name**: the name of the entity.
- **hash**: an internal identifier for the entity that is used in other API calls.
- **type**: identifies the kind of entity. One of: file, machine, project, server, user, volume, printer, share, resource, website, or ip.
- **risk**: the current risk of the entity.
- **showRiskBall**: specifies whether to show a visual indicator of the risk.

- **hover**

Additional text to use for hovering.

```
"... the user {{#hover title=\"accessed in some way\"}} touched {{/hover}}
27 projects ..."
```

This text provides a hint to the user interface that additional disclosure text is available. The text from the title field could be shown, for example, when the user hovers over the highlighted text.


Use the API with the Swagger UI

You can use Swagger UI to familiarize yourself with the API. In the Swagger UI, you can see all the endpoints, their parameters, and sample responses.



Note: By default, access to the APIs is disabled. To request access to the APIs, contact Micro Focus Customer Support at <https://softwaresupport.softwaregrp.com/>. After the access has been provided, only a user with an Admin role can call the API endpoints.

To access the Swagger UI:

1. In a web browser, log in to Intelligence with an Admin role .
2. Click  , point to **API Documentation** >, then select the desired API in the drop-down list.
Swagger for the selected API opens in a new browser window.
3. Click a category (such as **actions** or **tenants**) to expand it.
The endpoints that are part of that category are listed.
4. Click an endpoint to show all its details. You can call an endpoint by clicking **Try it out!**, filling in the **Parameters** section (if required by the endpoint), and then clicking **Execute**.

Example: Call an Endpoint

In this example, we will call the `info/build` endpoint.

1. In the Swagger UI, expand **info**, and then expand **GET /info/build**.
2. Scroll down to the **Response Messages** section, and then Click **Try it out!**.
3. The response is displayed in the **Response Body** section.

Tuning API Reference

Version: 6.4.5

BasePath: `/interset/tuning`

Alert Templates

POST `/{tid}/alert_templates`

Consumes

- `application/json`

Produces

- `application/json`

Path parameters

- **tid** (required)
Tenant ID

Request body

[AlertTemplate](#)

Responses

default

successful operation

GET `/{tid}/alert_templates/{anomalyType}/{did}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **anomalyType** (required)
Analytics Anomaly Type (i.e. 200)
- **did** (required)
Data Identifier

Return type

[AlertTemplate](#)

Example data

Content-Type: application/json

```
{
  "genericSearchQuery" : "genericSearchQuery",
  "reconSearchQuery" : "reconSearchQuery",
  "unitName" : "unitName",
  "anomalyType" : "anomalyType",
  "reconStartTime" : "reconStartTime",
  "tid" : "tid",
  "templatesAlert" : "templatesAlert",
  "reconEndTime" : "reconEndTime",
  "unitType" : "unitType",
  "hasAggregatedIdentifiers" : true,
  "genericTimeRangeQuery" : "genericTimeRangeQuery",
  "datasource" : "datasource",
  "threatDescription" : "threatDescription",
  "familyName" : "familyName",
  "unitDescription" : "unitDescription",
  "contextType" : "contextType",
  "threatName" : "threatName",
  "templatesThreat" : "templatesThreat",
  "sqlSearchQuery" : "sqlSearchQuery",
  "templatesFamily" : "templatesFamily",
  "templatesTooltip" : "templatesTooltip",
  "bucketSize" : "bucketSize",
  "did" : 0,
  "templatesTeaser" : "templatesTeaser"
}
```

Responses

200

successful operation

Anomaly Meta

POST /{tid}/anomaly_meta

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Request body

[AnomalyMeta](#)

Responses

default

successful operation

DELETE /{tid}/anomaly_meta/{anomalyType}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **anomalyType** (required)
Analytics Anomaly Type (i.e. 200)

Responses

default

successful operation

GET /{tid}/anomaly_meta/{anomalyType}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **anomalyType** (required)
Analytics Anomaly Type (i.e. 200)

Return type

[AnomalyMeta](#)

Example data

Content-Type: application/json

```
{
  "anomalyType" : 0,
  "timeBucket" : "timeBucket",
  "tid" : "tid"
}
```

Responses

200

successful operation

GET /{tid}/anomaly_meta

Produces

- application/json

Path parameters

- **tid** (required)

Tenant ID

Return type

array[[AnomalyMeta](#)]

Example data

Content-Type: application/json

```
[ {
  "anomalyType" : 0,
  "timeBucket" : "timeBucket",
  "tid" : "tid"
}, {
  "anomalyType" : 0,
  "timeBucket" : "timeBucket",
  "tid" : "tid"
} ]
```

Responses

200

successful operation

PUT `/{tid}/anomaly_meta/{anomalyType}`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **anomalyType** (required)
Analytics Anomaly Type (i.e. 200)

Request body

[AnomalyMeta](#)

Responses

default

successful operation

DELETE /{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key

- **tag** (required)
Tag Value

Responses

default

successful operation

GET /{tid}/did_tags

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Return type

array[[DidTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
```

```
"ds" : "ds"  
} ]
```

Responses

200

successful operation

GET /{tid}/did_tags/{ds}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source

Return type

array[[DidTag](#)]

Example data

Content-Type: application/json

```
[ {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
}, {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",
```

```
"tid" : "tid",  
"did" : 0,  
"ds" : "ds"  
} ]
```

Responses

200

successful operation

GET /{tid}/did_tags/{ds}/{did}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier

Return type

array[[DidTag](#)]

Example data

Content-Type: application/json

```
[ {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
}
```

```
}, {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
} ]
```

Responses

200

successful operation

GET `/{tid}/did_tags/{ds}/{did}/{type}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')

Return type

array[[DidTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET `/{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)

Tag Key

- **tag** (required)

Tag Value

Return type

[DidTag](#)

Example data

Content-Type: application/json

```
{
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

Responses

200

successful operation

GET `/{tid}/did_tags/{ds}/{did}/{type}/{identifier}`

Produces

- application/json

Path parameters

- **tid** (required)

Tenant ID

- **ds** (required)

Data Source

- **did** (required)

Data Identifier

- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key

Return type

array[[DidTag](#)]

Example data

Content-Type: application/json

```
[ {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
}, {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
} ]
```

Responses

200

successful operation

PUT `/{tid}/did_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key
- **tag** (required)
Tag Value

Request body

[DidTag](#)

Responses

default

successful operation

Entity Mappings

POST `/{tid}/entity_mappings`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Request body

EntityMapping

Responses

default

successful operation

DELETE /{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **entityType** (required)
Entity Type
- **entityId** (required)
Entity ID

Responses

default

successful operation

GET `/{tid}/entity_mappings/{ds}/{did}/{entityType}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **entityType** (required)
Entity Type

Return type

array[[EntityMapping](#)]

Example data

Content-Type: application/json

```
[ {  
  "mapping" : "mapping",  
  "entityType" : "entityType",  
  "entityId" : "entityId",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
}, {
```

```
"mapping" : "mapping",  
"entityType" : "entityType",  
"entityId" : "entityId",  
"tid" : "tid",  
"did" : 0,  
"ds" : "ds"  
} ]
```

Responses

200

successful operation

GET /{tid}/entity_mappings/{ds}/{did}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier

Return type

array[[EntityMapping](#)]

Example data

Content-Type: application/json

```
[ {  
  "mapping" : "mapping",  
  "entityType" : "entityType",  
  "entityId" : "entityId",
```

```
"tid" : "tid",
"did" : 0,
"ds" : "ds"
}, {
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET /{tid}/entity_mappings/{ds}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source

Return type

array[[EntityMapping](#)]

Example data

Content-Type: application/json

```
[ {
  "mapping" : "mapping",
```

```

    "entityType" : "entityType",
    "entityId" : "entityId",
    "tid" : "tid",
    "did" : 0,
    "ds" : "ds"
  }, {
    "mapping" : "mapping",
    "entityType" : "entityType",
    "entityId" : "entityId",
    "tid" : "tid",
    "did" : 0,
    "ds" : "ds"
  } ]

```

Responses

200

successful operation

GET /{tid}/entity_mappings

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Return type

array[[EntityMapping](#)]

Example data

Content-Type: application/json

```

[ {
  "mapping" : "mapping",
  "entityType" : "entityType",

```



```
"entityId" : "entityId",
"tid" : "tid",
"did" : 0,
"ds" : "ds"
}, {
"mapping" : "mapping",
"entityType" : "entityType",
"entityId" : "entityId",
"tid" : "tid",
"did" : 0,
"ds" : "ds"
} ]
```

Responses

200

successful operation

GET `/{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **entityType** (required)
Entity Type
- **entityId** (required)
Entity ID

Return type

[EntityMapping](#)

Example data

Content-Type: application/json

```
{
  "mapping" : "mapping",
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}
```

Responses

200

successful operation

PUT `/{tid}/entity_mappings/{ds}/{did}/{entityType}/{entityId}`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)

Data Identifier

- **entityType** (required)

Entity Type

- **entityId** (required)

Entity ID

Request body

[EntityMapping](#)

Responses

default

successful operation

Entity Tags

POST /{tid}/entity_tags

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)

Tenant ID

Request body

[EntityTag](#)

Responses

default

successful operation

DELETE `/{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key
- **tag** (required)
Tag Value

Responses

default

successful operation

GET `/{tid}/entity_tags`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Return type

array[[EntityTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET `/{tid}/entity_tags/{ds}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source

Return type

array[[EntityTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET `/{tid}/entity_tags/{ds}/{did}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier

Return type

array[[EntityTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET `/{{tid}}/entity_tags/{{ds}}/{{did}}/{{type}}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')

Return type

array[[EntityTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```


Responses

200

successful operation

GET `/{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key
- **tag** (required)
Tag Value

Return type

[EntityTag](#)

Example data

Content-Type: application/json

```
{  
  "identifier" : "identifier",  
  "tag" : "tag",
```

```
"type" : "type",  
"tid" : "tid",  
"did" : 0,  
"ds" : "ds"  
}
```

Responses

200

successful operation

GET `/{tid}/entity_tags/{ds}/{did}/{type}/{identifier}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key

Return type

array[[EntityTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

PUT `/{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier

- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key
- **tag** (required)
Tag Value

Request body

[EntityTag](#)

Responses

default

successful operation

Example Anomalies

GET `/{tid}/alert_templates/example/{anomaly_type}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **anomaly_type** (required)
Analytics Anomaly Type (i.e. 200)

Return type

[ExampleAnomaly](#)

Example data

Content-Type: application/json

```
{
  "exampleEndTimestamp" : "exampleEndTimestamp",
  "exampleEntityType" : "exampleEntityType",
  "exampleEntityHash" : "exampleEntityHash",
  "exampleEntityName" : "exampleEntityName",
  "exampleRisk" : 6.027456183070403,
  "exampleProbability" : 1.4658129805029452,
  "exampleObserved" : 5.962133916683182,
  "exampleBaseline" : 5.637376656633329,
  "exampleIdHash" : "exampleIdHash",
  "tid" : "tid",
  "exampleTimestamp" : "exampleTimestamp",
  "exampleRelation" : "exampleRelation",
  "exampleIdName" : "exampleIdName",
  "exampleDid" : 0,
  "exampleAssociatedEntities" : "exampleAssociatedEntities",
  "exampleAnomalyType" : "exampleAnomalyType",
  "exampleIdType" : "exampleIdType"
}
```

Responses

200

successful operation

POST /{tid}/importance

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Request body

Importance

Responses

default

successful operation

DELETE /{tid}/importance/{entityType}/{entityId}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **entityType** (required)
Entity Type
- **entityId** (required)
Entity ID

Responses

default

successful operation

GET /{tid}/importance/{entityType}/{entityId}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **entityType** (required)
Entity Type
- **entityId** (required)
Entity ID

Return type

Importance

Example data

Content-Type: application/json

```
{
  "score" : 0.8008281904610115,
  "entityType" : "entityType",
  "entityId" : "entityId",
  "tid" : "tid",
  "timestamp" : "2000-01-23T04:56:07.000+00:00"
}
```

Responses

200

successful operation

GET /{tid}/importance

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Return type

array[[Importance](#)]

Example data

Content-Type: application/json

```
[ {  
  "score" : 0.8008281904610115,  
  "entityType" : "entityType",  
  "entityId" : "entityId",  
  "tid" : "tid",  
  "timestamp" : "2000-01-23T04:56:07.000+00:00"  
}, {  
  "score" : 0.8008281904610115,  
  "entityType" : "entityType",  
  "entityId" : "entityId",  
  "tid" : "tid",  
  "timestamp" : "2000-01-23T04:56:07.000+00:00"  
} ]
```

Responses

200

successful operation

GET /{tid}/importance/{entityType}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **entityType** (required)
Entity Type

Return type

array[[Importance](#)]

Example data

Content-Type: application/json

```
[ {  
  "score" : 0.8008281904610115,  
  "entityType" : "entityType",  
  "entityId" : "entityId",  
  "tid" : "tid",  
  "timestamp" : "2000-01-23T04:56:07.000+00:00"  
}, {  
  "score" : 0.8008281904610115,  
  "entityType" : "entityType",  
  "entityId" : "entityId",  
  "tid" : "tid",  
  "timestamp" : "2000-01-23T04:56:07.000+00:00"  
} ]
```

Responses

200

successful operation

PUT `/{tid}/importance/{entityType}/{entityId}`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **entityType** (required)
Entity Type
- **entityId** (required)
Entity ID

Request body

Importance

Responses

default

successful operation

Parameters

POST /{tid}/parameters

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Request body

Parameter

Responses

default

successful operation

DELETE `/{tid}/parameters/{name}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **name** (required)
Parameter Name

Responses

default

successful operation

GET `/{tid}/parameters/{name}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **name** (required)
Parameter Name

Return type

[Parameter](#)

Example data

Content-Type: application/json

```
{  
  "name" : "name",  
  "value" : 0.8008281904610115,  
  "tid" : "tid"  
}
```

Responses

200

successful operation

GET /{tid}/parameters

Produces

- application/json

Path parameters

- **tid** (required)

Tenant ID

Return type

array[[Parameter](#)]

Example data

Content-Type: application/json

```
[ {  
  "name" : "name",  
  "value" : 0.8008281904610115,  
  "tid" : "tid"  
}, {  
  "name" : "name",  
  "value" : 0.8008281904610115,  
  "tid" : "tid"  
} ]
```

Responses

200

successful operation

PUT /{tid}/parameters/{name}

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **name** (required)
Parameter Name

Request body

[Parameter](#)

Responses

default

successful operation

Relation Tags

POST `/tid/relation_tags`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Request body

[RelationTag](#)

Responses

default

successful operation

DELETE `/{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key
- **tag** (required)
Tag Value

Responses

default

successful operation

GET `/{tid}/relation_tags`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Return type

array[[RelationTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET `/{tid}/relation_tags/{ds}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source

Return type

array[[RelationTag](#)]

Example data

Content-Type: application/json

```
[ {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
}, {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
} ]
```

Responses

200

successful operation

GET `/{tid}/relation_tags/{ds}/{did}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier

Return type

array[[RelationTag](#)]

Example data

Content-Type: application/json

```
[ {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
}, {  
  "identifier" : "identifier",  
  "tag" : "tag",  
  "type" : "type",  
  "tid" : "tid",  
  "did" : 0,  
  "ds" : "ds"  
} ]
```

Responses

200

successful operation

GET `/{tid}/relation_tags/{ds}/{did}/{type}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')

Return type

array[[RelationTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET `/{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key
- **tag** (required)
Tag Value

Return type

[RelationTag](#)

Example data

Content-Type: application/json

```
{  
  "identifier" : "identifier",  
  "tag" : "tag",
```

```
"type" : "type",  
"tid" : "tid",  
"did" : 0,  
"ds" : "ds"  
}
```

Responses

200

successful operation

GET `/{tid}/relation_tags/{ds}/{did}/{type}/{identifier}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier
- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key

Return type

array[[RelationTag](#)]

Example data

Content-Type: application/json

```
[ {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "identifier" : "identifier",
  "tag" : "tag",
  "type" : "type",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

PUT `/{tid}/relation_tags/{ds}/{did}/{type}/{identifier}/{tag}`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **ds** (required)
Data Source
- **did** (required)
Data Identifier

- **type** (required)
Tag Type (i.e. 'did')
- **identifier** (required)
Tag Key
- **tag** (required)
Tag Value

Request body

[RelationTag](#)

Responses

default

successful operation

Violations

GET `/{tid}/violations/{violationName}`

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **violationName** (required)
Alert Name

Return type

array[[AlertsMeta](#)]

Example data

Content-Type: application/json

```
[ {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

GET /{tid}/violations

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Return type

array[[AlertsMeta](#)]

Example data

Content-Type: application/json

```
[ {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
}, {
  "alertType" : "alertType",
  "alertName" : "alertName",
  "anomalyType" : 6,
  "timeBucket" : "timeBucket",
  "tid" : "tid",
  "did" : 0,
  "ds" : "ds"
} ]
```

Responses

200

successful operation

POST /{tid}/violations/register

Register Violation.

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Request body

[AlertsMetaViolations](#)

Responses

default

successful operation

Weights

POST `/{tid}/weights`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID

Request body

[Weight](#)

Responses

default

successful operation

DELETE /{tid}/weights/{did}/{anomalyType}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **did** (required)
Data Identifier
- **anomalyType** (required)
Analytics Anomaly Type (i.e. 200)

Responses

default

successful operation

GET /{tid}/weights/{did}/{anomalyType}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **did** (required)
Data Identifier
- **anomalyType** (required)
Analytics Anomaly Type (i.e. 200)

Return type

[Weight](#)

Example data

Content-Type: application/json

```
{
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
}
```

Responses

200

successful operation

GET /{tid}/weights

Produces

- application/json

Path parameters

- **tid** (required)

Tenant ID

Return type

array[[Weight](#)]

Example data

Content-Type: application/json

```
[ {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
}, {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
} ]
```

Responses

200

successful operation

GET /{tid}/weights/{did}

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **did** (required)
Data Identifier

Return type

array[[Weight](#)]

Example data

Content-Type: application/json

```
[ {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
}, {
  "anomalyType" : 6,
  "importance" : 5.637376656633329,
  "weight" : 1.4658129805029452,
  "probabilityThreshold" : 2.3021358869347655,
  "tid" : "tid",
  "did" : 0,
  "defaultWeight" : 5.962133916683182
} ]
```

Responses

200

successful operation

PUT `/{tid}/weights/{did}/{anomalyType}`

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
Tenant ID
- **did** (required)
Data Identifier
- **anomalyType** (required)
Analytics Anomaly Type (i.e. 200)

Request body

Weight

Responses

default

successful operation

Models

AlertTemplate

- **tid** -- String
- **did** -- Integer
Format: int32
- **anomalyType** -- String

- **datasource** -- String
- **threatName** -- String
- **threatDescription** -- String
- **familyName** -- String
- **unitName** -- String
- **unitType** -- String
- **unitDescription** -- String
- **templatesTeaser** -- String
- **templatesAlert** -- String
- **templatesThreat** -- String
- **templatesFamily** -- String
- **templatesTooltip** -- String
- **reconSearchQuery** -- String
- **reconStartTime** -- String
- **reconEndTime** -- String
- **bucketSize** -- String
- **contextType** -- String
- **genericSearchQuery** -- String
- **genericTimeRangeQuery** -- String
- **sqlSearchQuery** -- String
- **hasAggregatedIdentifiers** -- Boolean

AlertsMeta

- **tid** -- String
- **ds** -- String
- **did** -- Integer

Format: int32

- **alertType** -- String
- **alertName** -- String
- **timeBucket** -- String
- **anomalyType** -- Integer
Format: int32

AlertsMetaSimple

- **tid** -- String
- **ds** -- String
- **did** -- Integer
Format: int32
- **alertName** -- String
- **timeBucket** -- String

AlertsMetaViolations

- **tid** -- String
- **ds** -- String
- **did** -- Integer
Format: int32
- **alertName** -- String
- **timeBucket** -- String
- **severity** -- String

AnomalyMeta

- **tid** -- String
- **anomalyType** -- Integer
Format: int32
- **timeBucket** -- String

- **tid** -- String
- **ds** -- String
- **did** -- Integer
Format: int32
- **type** -- String
- **identifier** -- String
- **tag** -- String

EntityMapping

- **tid** -- String
- **ds** -- String
- **did** -- Integer
Format: int32
- **entityType** -- String
- **entityId** -- String
- **mapping** -- String

EntityTag

- **tid** -- String
- **ds** -- String
- **did** -- Integer

Format: int32

- **type** -- String
- **identifier** -- String
- **tag** -- String

ExampleAnomaly

- **tid** -- String
- **exampleAnomalyType** -- String
- **exampleDid** -- Integer
Format: int32
- **exampleTimestamp** -- String
- **exampleRisk** -- Double
Format: double
- **exampleProbability** -- Double
Format: double
- **exampleObserved** -- Double
Format: double
- **exampleBaseline** -- Double
Format: double
- **exampleRelation** -- String
- **exampleEntityName** -- String
- **exampleEntityHash** -- String
- **exampleEntityType** -- String
- **exampleIdName** -- String
- **exampleIdHash** -- String
- **exampleIdType** -- String
- **exampleEndTimestamp** -- String
- **exampleAssociatedEntities** -- String

Importance

- **tid** -- String
- **entityType** -- String
- **entityId** -- String
- **score** -- Double
Format: double
- **timestamp** -- Date
Format: date-time

Parameter

- **tid** -- String
- **name** -- String
- **value** -- Double
Format: double

RelationTag

- **tid** -- String
- **ds** -- String
- **did** -- Integer
Format: int32
- **type** -- String
- **identifier** -- String
- **tag** -- String

Weight

- **tid** -- String
- **did** -- Integer
Format: int32
- **anomalyType** -- Integer
Format: int32
- **weight** -- Double
Format: double
- **defaultWeight** -- Double
Format: double
- **importance** -- Double
Format: double
- **probabilityThreshold** -- Double
Format: double

Analytics API Reference

Version: 6.4.5

BasePath: /interset/api

actions

POST /actions/login

Log in

Authenticates and creates a new session for the specified user identifier and password. Returns a JSON structure containing an access token and the token type.

Consumes

- application/json

Produces

- application/json

Request body

[ApiCredentials](#)

Return type

[LoginResponse](#)

Example data

Content-Type: application/json

```
{
  "access_token" : "802BR4y-kaj0PE4agOR_d4RaE-Ja",
  "token_type" : "Bearer"
}
```

Responses

200

successful operation

GET /actions/logoff

Log off

Ends the specified user session. Expects an Authorization header containing the string "<token_type>: <access_token>".The token_type is typically "Bearer".

Consumes

- application/json

Produces

- application/json

Request headers

- **Authorization** (optional) -- String

Return type

[ApiAction](#)

Example data

Content-Type: application/json

```
{
  "success" : true,
  "detail" : "logged off"
}
```

Responses

200

successful operation

GET /actions/logoff/saml

Log off (SAML)

Expects an Authorization header containing the string "<token_type>: <access_token>". You can get both of these using the /actions/login/saml method. The token_type is typically "Bearer".

This method redirects requests to the SAML logout URL.

Consumes

- application/json

Produces

- application/json

Request headers

- **Authorization** (optional) -- String

Query parameters

- **relayState** (optional)

Responses

default

successful operation

GET /actions/login/oauth2

Login (OAuth2)

Login API for OAuth2

Consumes

- application/json

Produces

- application/json

Query parameters

- **relayState** (optional)

Responses

default

successful operation

GET /actions/login/oauth2/callback

CallBack URI (OAuth2)

This is callback handler which is registered with OAuth2 provider and this handler will be called with authcode and state info

Consumes

- application/json

Produces

- application/json

Query parameters

- **code** (optional)
- **state** (optional)

Responses

default

successful operation

GET /actions/logoff/oauth2

Log off (OAuth2)

Revokes refresh token and invalidates all the sessions and cookies

Consumes

- application/json

Produces

- application/json

Request headers

- **Authorization** (optional) -- String

Query parameters

- **relayState** (optional)

Responses

default

successful operation

GET /actions/login/oauth2/renew

Renew Token (OAuth2)

Generates new access token using refresh token. Sets Interset Cookie and Authorization header with new access token

Consumes

- application/json

Produces

- application/json

Request headers

- **Authorization** (optional) -- String

Responses

default

successful operation

GET /actions/login/saml

Get SAML login page

Returns an HTML document that loads a SAML login page and redirects the user to the requested path, if that path is valid.

Example Response (Status 200)

```
<html><head></head><body><form id='TheForm'
action='https://company.okta.com/app/investigator/katex9fJY47c0Kh7ij90/sso/saml'
method='POST'><input type='hidden' id='SAMLRequest' name='SAMLRequest'
value='PD94bWwgdmhbWwycDbolj0iMS4wIiBlbmNvZGluZz1Vyc2lvbKPHNjBdXR0iVVRGLTgiPz4cXV1
c3QgQXNzZXJ0aw9uQ29uc3VtZXJtZXJ2aWN1VWJMPStJodHRwczovL3FhLWNvczcyLWNUb2RlLmFk
LmludGVyc2V0LmNvbS9hcGkvYWw0aw9ucy9sb2dpci9zYW1sL3NzbyIgSUQ9InphODkwYjg5My0z
ODFhLTQ3MwQTYTZkOS05NzVkn2EwNT11NmIiIElzc3VlSW5zdGFudD0iMjAxNy0wOS0yOVQxOToz
NTowMC4yMjlaIiBQcm90b2NvbEJpbmRpbmc9InVybjpvYXNpczpuYW11czp0YzptQU1MOjIuMDpi
aw5kaW5nczplVFRQLVBPU1QiIFZlcnNpb249IjIuMCJgeG1sbnM6c2FtbDJwPSJ1cm46b2FzaXM6
bmFtZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wiPjxzYW1sMjpwMjIzZXIgeG1sbnM6c2FtbDI9InVy
bjpvYXNpczpuYW11czp0YzptQU1MOjIuMDphc3NlcnRpb24iPkIudmVzdGlnYXRvcjwvc2FtbDI6
SXNzdWVyPjxzYW1sMnA6TmFtZU1EUG9saWN5IEZvcmlhdD0idXJuOm9hc2lzOm5hbWVzOnRjO1NB
TUw6MS4xOm5hbWVpZC1mb3JtYXQ6dw5zcGVjaWZpZWQilz48L3NhbWwycDpBdXR0b1JlcXVlc3Q+' /><input
type='hidden' id='RelayState' name='RelayState' value='/interset' /></form><script
type='text/javascript'>document.getElementById('TheForm').submit
();</script></body></html>
```

Consumes

- application/json

Produces

- application/json

Query parameters

- **relayState** (optional)
The path where the user should be redirected once authenticated.

Responses

default

successful operation

POST /actions/login/saml/sso

Log in (SAML SSO)

Expects an IDP generated SAML response. Processes a signed SAML response.

Consumes

- application/x-www-form-urlencoded

Produces

- application/json

Form parameters

- **SAMLResponse** (optional)
- **RelayState** (optional)

The path where the user should be redirected once authenticated.

Responses

default

successful operation

dashboards{tenantId}

POST /dashboards/{tid}

Add a dashboard

Creates a new dashboard for the currently logged-in user.

Example Request Body

```
{
  "doc":{"title":"Overall Risk 2","layouts":[{"x":0,"y":0,"w":3,"h":16,"setting":
{"panelName":"MatrixVisualization"}]}},
  "description":"This is my second dashboard",
  "name":"Overall Risk 2",
  "private":false
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request body

[ApiSimpleDashboard](#)

Return type

[ApiDashboard](#)

Example data

Content-Type: application/json

```
{
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
}
```

Responses

200

successful operation

PUT /dashboards/{tid}/tags/{id}

Attach a tag to a dashboard

Attaches a new tag

Example Request Body

```
{  
  "name": "newTag",  
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)
The dashboard ID.

Request body

[ApiSimpleDashboardTag](#)

Responses

```
default
```

successful operation

DELETE /dashboards/{tid}/tags/{id}

Detach tag from dashboard

Removes specified tag from dashboard

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)

Responses

default

successful operation

GET /dashboards/{tid}/{id}

Get a dashboard

Returns the JSON representation of the dashboard with the specified ID.

Example Response (Status 200)

```
{
  "doc": {"title": "Overall Risk 2", "layouts": [{"x": 0, "y": 0, "w": 3, "h": 16, "setting": {"panelName": "MatrixVisualization"}}]},
  "name": "Overall Risk 2",
  "description": "This is my second dashboard",
  "tid": "0",
  "userId": "admin",
  "id": 78,
  "lastModifiedBy": "admin",
  "creationDate": "2018-11-22",
  "lastModifiedDate": "2018-11-22",
  "home": null,
  "private": false
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)
The dashboard ID.

Return type

[ApiDashboard](#)

Example data

Content-Type: application/json

```
{
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
}
```

Responses

200

successful operation

GET /dashboards/{tid}

Get a list of dashboards

Returns all public dashboards for the tenant, as well as the logged-in user's private dashboards.

Example Response (Status 200)

```
[
  {
    "doc":null,
    "name":"Overall Risk 2",
    "description":"description":"This is my second dashboard",
    "tid":null,
    "userId":"admin",
    "id":78,
    "lastModifiedBy":"admin",
    "creationDate":"2018-11-22",
    "lastModifiedDate":"2018-11-22",
    "home":false,
    "tags":[
      {
        "name":"addedTag",
        "id":"4"
      }
    ],
    "private":false
  },
  {
    "doc":null,
    "name":"Breakdown Dashboard",
    "description":"description":"This is my breakdown dashboard",
    "tid":"0",
    "userId":"admin",
    "id":79,
    "lastModifiedBy":"admin",
    "creationDate":"2018-11-10",
    "lastModifiedDate":"2018-11-10",
    "home":true,
    "tags": [],
    "private":false
  }
]
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Return type

array[[ApiDashboard](#)]

Example data

Content-Type: application/json

```
[ {
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
}, {
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
  "doc" : "doc",
  "description" : "description",
  "id" : 0,
  "creationDate" : "2000-01-23T04:56:07.000+00:00",
  "userId" : "userId",
  "tid" : "tid",
  "home" : true,
  "tags" : [ {
    "name" : "recon",
```

```

    "id" : "46b489f7f46588c6"
  }, {
    "name" : "recon",
    "id" : "46b489f7f46588c6"
  } ]
} ]

```

Responses

200

successful operation

GET /dashboards/{tid}/home

Get home dashboard

Returns the JSON representation of the home dashboard for the logged-in user.

Example Response (Status 200)

```

{
  "doc":{"title":"Overall Risk 2","layouts":[{"x":0,"y":0,"w":3,"h":16,"setting":
{"panelName":"MatrixVisualization"}]}},
  "name":"Overall Risk 2",
  "description":"This is my second dashboard",
  "tid":"0",
  "userId":"admin",
  "id":78,
  "lastModifiedBy":"admin",
  "creationDate":"2018-11-22",
  "lastModifiedDate":"2018-11-22",
  "home":null,
  "private":false
}

```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Responses

default

successful operation

GET /dashboards/{tid}/tags

Get a list of tags

Gets all tags for the tenant

Example Request Body

```
[
  {
    "name": "Aiden",
    "id": "4"
  },
  {
    "name": "Bryan",
    "id": "2"
  }
]
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Return type

array[[ApiDashboardTag](#)]

Example data

Content-Type: application/json

```
[ {
  "name" : "recon",
  "id" : "46b489f7f46588c6"
```

```
}, {  
  "name" : "recon",  
  "id" : "46b489f7f46588c6"  
} ]
```

Responses

200

successful operation

DELETE /dashboards/{tid}/{id}

Delete a dashboard

Deletes the dashboard with the specified ID. You must have the permissions required to delete the specified dashboard.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)

Responses

default

successful operation

DELETE /dashboards/{tid}/home

Reset home dashboard

Resets the home dashboard for the currently logged-in user.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Responses

default

successful operation

PUT /dashboards/{tid}/home/{id}

Update home dashboard

Sets the dashboard with the specified ID to be the home dashboard for the logged-in user.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)
The dashboard ID.

Responses

default

successful operation

PUT /dashboards/{tid}/{id}

Update a dashboard

Updates the dashboard with the specified ID. You must have the permissions required to update the specified dashboard.

Example Request Body

```
{
  "doc": {"title": "Overall Risk 2", "layouts": [{"x": 0, "y": 0, "w": 3, "h": 16, "setting":
{"panelName": "MatrixVisualization"}]}},
  "description": "This is my second dashboard",
  "name": "Overall Risk 2",
  "private": false
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)

Request body

[ApiSimpleDashboard](#)

Return type

[ApiDashboard](#)

Example data

Content-Type: application/json

```
{
  "private" : true,
  "lastModifiedDate" : "2000-01-23T04:56:07.000+00:00",
  "lastModifiedBy" : "lastModifiedBy",
  "name" : "name",
}
```

```
"doc" : "doc",
"description" : "description",
"id" : 0,
"creationDate" : "2000-01-23T04:56:07.000+00:00",
"userId" : "userId",
"tid" : "tid",
"home" : true,
"tags" : [ {
  "name" : "recon",
  "id" : "46b489f7f46588c6"
}, {
  "name" : "recon",
  "id" : "46b489f7f46588c6"
} ]
}
```

Responses

200

successful operation

events{tenantId}

POST /events/{tid}/savedSearches

Add a saved search

Creates a new saved search for the currently logged-in user.

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request body

[ApiSavedSearches](#)

Return type

[ApiSavedSearchesResponse](#)

Example data

Content-Type: application/json

```
{
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columns" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
```

```
"long" : true,
"textual" : true,
"empty" : true,
"missingNode" : true,
"pojo" : true,
"number" : true,
"boolean" : true,
"null" : true,
"array" : true,
"binary" : true,
"containerNode" : true,
"short" : true,
"bigDecimal" : true,
"object" : true
},
"name" : "name",
"doc" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
  "bigInteger" : true,
  "nodeType" : "ARRAY",
  "float" : true,
  "int" : true,
  "long" : true,
  "textual" : true,
  "empty" : true,
  "missingNode" : true,
  "pojo" : true,
  "number" : true,
  "boolean" : true,
  "null" : true,
  "array" : true,
  "binary" : true,
  "containerNode" : true,
  "short" : true,
  "bigDecimal" : true,
  "object" : true
},
"columnsDraft" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
  "bigInteger" : true,
  "nodeType" : "ARRAY",
```

```
"float" : true,
"int" : true,
"long" : true,
"textual" : true,
"empty" : true,
"missingNode" : true,
"pojo" : true,
"number" : true,
"boolean" : true,
"null" : true,
"array" : true,
"binary" : true,
"containerNode" : true,
"short" : true,
"bigDecimal" : true,
"object" : true
},
"id" : 0
}
```

Responses

200

successful operation

GET /events/{tid}/savedSearches

Get the saved searches for one user

Return the saved searches for one user on a specific tenant.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Return type

array[[ApiSavedSearchesResponse](#)]

Example data

Content-Type: application/json

```
[ {
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columns" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
```

```
"binary" : true,
"containerNode" : true,
"short" : true,
"bigDecimal" : true,
"object" : true
},
"name" : "name",
"doc" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
  "bigInteger" : true,
  "nodeType" : "ARRAY",
  "float" : true,
  "int" : true,
  "long" : true,
  "textual" : true,
  "empty" : true,
  "missingNode" : true,
  "pojo" : true,
  "number" : true,
  "boolean" : true,
  "null" : true,
  "array" : true,
  "binary" : true,
  "containerNode" : true,
  "short" : true,
  "bigDecimal" : true,
  "object" : true
},
"columnsDraft" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
  "bigInteger" : true,
  "nodeType" : "ARRAY",
  "float" : true,
  "int" : true,
  "long" : true,
  "textual" : true,
  "empty" : true,
  "missingNode" : true,
  "pojo" : true,
  "number" : true,
  "boolean" : true,
```

```
"null" : true,
"array" : true,
"binary" : true,
"containerNode" : true,
"short" : true,
"bigDecimal" : true,
"object" : true
},
"id" : 0
}, {
"docDraft" : {
"integralNumber" : true,
"double" : true,
"valueNode" : true,
"floatingPointNumber" : true,
"bigInteger" : true,
"nodeType" : "ARRAY",
"float" : true,
"int" : true,
"long" : true,
"textual" : true,
"empty" : true,
"missingNode" : true,
"pojo" : true,
"number" : true,
"boolean" : true,
>null" : true,
"array" : true,
"binary" : true,
"containerNode" : true,
"short" : true,
"bigDecimal" : true,
"object" : true
},
"columns" : {
"integralNumber" : true,
"double" : true,
"valueNode" : true,
"floatingPointNumber" : true,
"bigInteger" : true,
"nodeType" : "ARRAY",
"float" : true,
"int" : true,
"long" : true,
"textual" : true,
"empty" : true,
"missingNode" : true,
```

```
"pojo" : true,
"number" : true,
"boolean" : true,
"null" : true,
"array" : true,
"binary" : true,
"containerNode" : true,
"short" : true,
"bigDecimal" : true,
"object" : true
},
"name" : "name",
"doc" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
  "bigInteger" : true,
  "nodeType" : "ARRAY",
  "float" : true,
  "int" : true,
  "long" : true,
  "textual" : true,
  "empty" : true,
  "missingNode" : true,
  "pojo" : true,
  "number" : true,
  "boolean" : true,
  "null" : true,
  "array" : true,
  "binary" : true,
  "containerNode" : true,
  "short" : true,
  "bigDecimal" : true,
  "object" : true
},
"columnsDraft" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
  "bigInteger" : true,
  "nodeType" : "ARRAY",
  "float" : true,
  "int" : true,
  "long" : true,
  "textual" : true,
```

```
"empty" : true,  
"missingNode" : true,  
"pojo" : true,  
"number" : true,  
"boolean" : true,  
"null" : true,  
"array" : true,  
"binary" : true,  
"containerNode" : true,  
"short" : true,  
"bigDecimal" : true,  
"object" : true  
},  
"id" : 0  
} ]
```

Responses

200

successful operation

DELETE /events/{tid}/savedSearches/{id}

Delete a saved search

Deletes the saved search with the specified ID. You must have the permissions required to delete the specified saved search.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)

Responses

default

successful operation

DELETE /events/{tid}/savedSearches/{id}/draft

Removes a saved search draft

Deletes the draft for the saved search with the specified ID.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)

Responses

default

successful operation

PUT /events/{tid}/savedSearches/{id}

Update a saved search

Updates the saved search with the specified ID. You must have the permissions required to update the specified saved search.

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

- **id** (required)

Request body

[ApiSavedSearches](#)

Return type

[ApiSavedSearchesResponse](#)

Example data

Content-Type: application/json

```
{
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columns" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
```

```
"float" : true,
"int" : true,
"long" : true,
"textual" : true,
"empty" : true,
"missingNode" : true,
"pojo" : true,
"number" : true,
"boolean" : true,
"null" : true,
"array" : true,
"binary" : true,
"containerNode" : true,
"short" : true,
"bigDecimal" : true,
"object" : true
},
"name" : "name",
"doc" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
  "bigInteger" : true,
  "nodeType" : "ARRAY",
  "float" : true,
  "int" : true,
  "long" : true,
  "textual" : true,
  "empty" : true,
  "missingNode" : true,
  "pojo" : true,
  "number" : true,
  "boolean" : true,
  "null" : true,
  "array" : true,
  "binary" : true,
  "containerNode" : true,
  "short" : true,
  "bigDecimal" : true,
  "object" : true
},
"columnsDraft" : {
  "integralNumber" : true,
  "double" : true,
  "valueNode" : true,
  "floatingPointNumber" : true,
```

```
"bigInteger" : true,  
"nodeType" : "ARRAY",  
"float" : true,  
"int" : true,  
"long" : true,  
"textual" : true,  
"empty" : true,  
"missingNode" : true,  
"pojo" : true,  
"number" : true,  
"boolean" : true,  
"null" : true,  
"array" : true,  
"binary" : true,  
"containerNode" : true,  
"short" : true,  
"bigDecimal" : true,  
"object" : true  
},  
"id" : 0  
}
```

Responses

200

successful operation

PUT /events/{tid}/savedSearches/{id}/draft

Replace the draft for one saved search

Updates the draft for the saved search with the specified ID.

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)

Request body

[ApiSavedSearchesDraft](#)

Return type

[ApiSavedSearchesDraft](#)

Example data

Content-Type: application/json

```
{
  "docDraft" : {
    "integralNumber" : true,
    "double" : true,
    "valueNode" : true,
    "floatingPointNumber" : true,
    "bigInteger" : true,
    "nodeType" : "ARRAY",
    "float" : true,
    "int" : true,
    "long" : true,
    "textual" : true,
    "empty" : true,
    "missingNode" : true,
    "pojo" : true,
    "number" : true,
    "boolean" : true,
    "null" : true,
    "array" : true,
    "binary" : true,
    "containerNode" : true,
    "short" : true,
    "bigDecimal" : true,
    "object" : true
  },
  "columnsDraft" : {
```

```
"integralNumber" : true,  
"double" : true,  
"valueNode" : true,  
"floatingPointNumber" : true,  
"bigInteger" : true,  
"nodeType" : "ARRAY",  
"float" : true,  
"int" : true,  
"long" : true,  
"textual" : true,  
"empty" : true,  
"missingNode" : true,  
"pojo" : true,  
"number" : true,  
"boolean" : true,  
"null" : true,  
"array" : true,  
"binary" : true,  
"containerNode" : true,  
"short" : true,  
"bigDecimal" : true,  
"object" : true  
}  
}
```

Responses

200

successful operation

info

GET /info/auth

Get authentication provider information

Returns information about enabled authentication provider(s).

Example Response (Status 200)

```
{  
  "ldap": false,  
}
```

```
"saml": true,  
"local": false  
}
```

Produces

- application/json

Responses

default

successful operation

GET /info/analysedEntities/{tid}

Get the number of entities that have been ingested and are available for analysis

Returns the number of availed entities in the dataset.

Example Response (Status 200)

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `entityType:users OR entityType:machines`):

- **entityType**: Allows filtering using the entityTypes (e.g., `entityType:users`)

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Query parameters

- **q** (optional)
Query filter.

Responses

default

successful operation

GET /info/deployment

Get deployment information

Returns information about deployment type.

Example Response (Status 200)

```
{
  "ldap": false,
  "saml": true,
  "local": false
}
```

Produces

- application/json

Responses

default

successful operation

GET /info/session

Get session information

Returns information about the current session.

Produces

- application/json

Return type

[SessionInfo](#)

Example data

Content-Type: application/json

```
{
  "extendedApi" : [ {
    "schema" : "schema",
    "prefix" : "prefix",
    "name" : "name",
    "description" : "description",
    "menu" : "menu",
    "permissionsByMethod" : {
      "key" : "ACCESS_INTELLIGENCE"
    }
  }, {
    "schema" : "schema",
    "prefix" : "prefix",
    "name" : "name",
    "description" : "description",
    "menu" : "menu",
    "permissionsByMethod" : {
      "key" : "ACCESS_INTELLIGENCE"
    }
  } ],
  "persistentSessions" : false,
  "permissions" : [ {
    "features" : "showTuning",
    "tenantName" : "Interaset",
    "tenantId" : "0",
    "permission" : "ACCESS_INTELLIGENCE,VIEW_INTELLIGENCE_RAW_EVENTS",
    "userId" : "camilla"
  }, {
    "features" : "showTuning",
    "tenantName" : "Interaset",
    "tenantId" : "0",
    "permission" : "ACCESS_INTELLIGENCE,VIEW_INTELLIGENCE_RAW_EVENTS",
    "userId" : "camilla"
  } ],
  "userDisplayName" : "Camilla Ferguson",
  "swaggerEndpoints" : {
    "key" : "swaggerEndpoints"
  },
  "analyticsTuningAvailable" : true,
  "disableTenantManagement" : false,
  "accessToken" : "FFvoDf8VkeKITR-L3z3xU_uKZxrT",
  "userId" : "camilla"
}
```

Responses

200

successful operation

GET /info/build

Get version information

Returns information about this Interset build.

Example Response (Status 200)

```
{
  "Api-Current-Version": "6.3.0",
  "Build-Date": "2018-04-27T03:01:37Z",
  "Build-Number": "6.3.0.102",
  "Archiver-Version": "Plexus Archiver",
  "Built-By": "root",
  "Version": "6.3.0-SNAPSHOT",
  "Manifest-Version": "1.0",
  "Git-Commit": "b72836125ba95d855397b7fa63e50847f3fe255a",
  "Main-Class": "com.interset.reporting.InvestigatorApplication",
  "Git-Branch": "6.3.0",
  "Application": "com.interset.reporting",
  "Name": "reporting",
  "Created-By": "Apache Maven 3.3.9",
  "Build-Jdk": "1.8.0_92",
  "Api-Deprecated-Version": "5.9.0"
}
```

Produces

- application/json

Responses

default

successful operation

rawEvents{tenantId}

POST /rawEvents/{tid}/typeAhead

Auto-complete event field by column

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request body

[RawEventsTypeaheadRequest](#)

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /rawEvents/{tid}/csv

Get raw data as CSV

Download raw events in CSV format.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Query parameters

- **q** (optional)
Accepts a Kibana-type query against the applicable raw data. For example, (user: ("camilla")) AND (project:("csrv/re13/Auditor")).
- **ds** (optional)
Comma separated list of datasources against which to query. Default includes all.
- **count** (optional)
The maximum number of raw events to return.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET /rawEvents/{tid}

Get raw data as JSON

Download raw events in JSON format.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **q** (optional)
Accepts a Kibana-type query against the applicable raw data. For example, (user: ("camilla")) AND (project:("csrv/re13/Auditor")).
- **ds** (optional)
Comma separated list of datasources against which to query. Default includes all.
- **count** (optional)
The maximum number of raw events to return.
- **includeFields** (optional)
Should the fields be returned. If false, allFields and sortableFields will be omitted.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

POST /rawEvents/{tid}/graph

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request body

[RawEventsGraphRequest](#)

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

POST /rawEvents/{tid}/resolve

Get raw data as json or csv

Retrieve raw events in csv or json.

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request body

```
array[String]
```

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **format** (optional)
The format of the response. Can be json or csv.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET /rawEvents/{tid}/resolve/{id}

Get raw data as json or csv

Retrieve raw events in csv or json.

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **id** (required)
Event id

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **format** (optional)
The format of the response. Can be json or csv.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

POST /rawEvents/{tid}/search

Get an event stream that returns raw data as it's retrieved from backend storage

Stream raw events

Consumes

- application/json

Produces

- text/event-stream

Path parameters

- **tid** (required)
The tenant ID.

Request body

[RawEventsRequest](#)

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **count** (optional)
The maximum number of raw events to return.
- **includeFields** (optional)
Should the fields be returned. If false, allFields and sortableFields will be omitted.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **scrollId** (optional)
The scrollId from the previous request. Use this scrollId to get subsequent results.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)

End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

search{tenantId}

GET /search/{tid}/{rollupLevel}/breakdown/risk

Get risk breakdown for alerts/anomalies

Gets the number of anomalies or alerts for each risk breakdown (low, medium, high, extreme).

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "extreme": 38,
    "high": 433,
    "low": 231422,
    "medium": 2103
  },
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid:** Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user:** Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk:** Allows filtering by risk level (low, medium, high, extreme).
- **anomalies:** Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.
- **rollupLevel** (required)
The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **minRisk** (optional)
Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.
- **maxRisk** (optional)
Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.
- **q** (optional)
Query filter.
- **scType** (optional)
Scaled contribution type. Always use `risk`; `contribution` is deprecated.
- **sc** (optional)
Scaled contribution. Deprecated; use `minRisk`.
- **ts** (optional)

Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/{rollupLevel}

Get anomalies/alerts/aggregates for the selected level

Returns anomalies, alerts, or aggregates for the selected rollup and for the specified tenant.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "id": "",
      "alertId": "",
      "datasource": "repo",
      "timestamp": 1393567200,
      "risk": 13,
      "contribution": 10,
      "significance": 88,
      "templates": {
        "threat": "",
        "family": "",
        "teaser": "",
        "alert": "",
        "tooltip": ""
      },
      "anomalyTypes": [
        11
      ],
      "numAnomalies": 2,
      "category": "Repository",
    }
  ]
}
```

```

    "bucketSize": "hourly",
    "rollupLevel": "alerts",
    "numChildren": 2,
    "parentId": "aggId1",
    "kibana": {
      "searchQuery": "",
      "indexName": ""
    },
    "contextAnomalyId": "",
    "contextType": "none",
    "tags": [
      {
        "id": "tagId1",
        "name": "foo",
        "source": "user",
        "createdAt": 1493453400000,
        "createdBy": "jp"
      },
      {
        "id": "tagId1",
        "name": "foo",
        "source": "user",
        "createdAt": 1493567200000,
        "createdBy": "sean"
      }
    ]
  },
],
"totalHits": 25,
"scrollId": "vabsjk5h24e1kdasjfojdabhgjk32b5b",
"cached": false
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **rollupLevel** (required)
The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **count** (optional)
count
- **sort** (optional)
Method of sorting alerts.
- **sortOrder** (optional)
Specifies the sort order of the results. Possible values are desc and asc.
- **riskSort** (optional)
Risk sort order in which to return entities.
- **minRisk** (optional)
Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.
- **maxRisk** (optional)
Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.
- **q** (optional)
Query filter.

- **markup** (optional)
Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, `{{ and }}`. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.
- **scrollId** (optional)
The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.
- **scType** (optional)
Scaled contribution type. Always use `risk`; `contribution` is deprecated.
- **sc** (optional)
Scaled contribution. Deprecated; use `minRisk`.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET /search/{tid}/{rollupLevel}/count

Get total count for rollup level

Gets the total number of aggregates, alerts, or anomalies for the specified tenant and rollup level.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
```



```
"count": 237086
},
"cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators `AND` and `OR` serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically `ORed`, and those concerning different entities are `ANDed`.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.
- **rollupLevel** (required)
The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **minRisk** (optional)
Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.
- **maxRisk** (optional)
Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.
- **q** (optional)
Query filter.
- **scType** (optional)
Scaled contribution type. Always use `risk`; `contribution` is deprecated.
- **sc** (optional)
Scaled contribution. Deprecated; use `minRisk`.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET /search/{tid}/{rollupLevel}/{rollupId}

Get anomaly/alert/aggregate for specified rollupId

Returns the anomaly, alert, or aggregate with the specified rollup ID (anomaly ID, alert ID, aggregate ID).

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "id": "ebea3079901fd4c1",
    "alertId": "ebea3079901fd4c1",
    "datasource": "repo",
    "timestamp": 1393453400,
    "risk": 8100,
    "contribution": 100,
    "significance": 88,
    "templates": {
      "threat": "",
      "family": "",
      "teaser": "",
      "alert": "",
      "tooltip": ""
    },
    "anomalyTypes": [
      11
    ],
    "numAnomalies": 2,
    "category": "Repository",
    "bucketSize": "hourly",
    "rollupLevel": "alerts",
    "numChildren": 2,
    "parentId": null,
    "kibana": {
      "searchQuery": "",
      "indexName": ""
    },
    "contextAnomalyId": "",
    "contextType": "none",
    "tags": [
      {
        "id": "tagId1",
        "name": "foo",
        "source": "user",
        "createdAt": 1493453400000,
        "createdBy": "jp"
      },
      {
        "id": "tagId1",
        "name": "foo",
        "source": "user",
        "createdAt": 1493567200000,
        "createdBy": "sean"
      }
    ]
  }
}
```

```

},
"totalHits": 25,
"cached": "false",
"scrollId": "vabsjk5h24e1kdasjfojdabhgjk32b5b"
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same entityType are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.
- **rollupLevel** (required)
The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.
- **rollupId** (required)
The ID of the aggregate, alert or anomaly to match.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **markup** (optional)

Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, `{{` and `}}`. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

- **riskSort** (optional)

Which risk score should be associated with an entity.

Responses

default

successful operation

GET /search/{tid}/controllers/authentications

Get authentication attempts

Provides an overview of the number of successful and failed authentication attempts made against servers.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "failed": 4,
    "succeeded": 45
  },
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.

- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

`default`

successful operation

GET /search/{tid}/{rollupLevel}/{rollupId}/context

Get context around an aggregate/alert/anomaly

Returns the context and statistics for the specified anomaly, alert, or aggregate.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "values": [
      {
        "key": "probability",
        "value": 33.0,
        "type": "percentage",
        "description": "Anomalousness",
        "displayName": ""
      }
    ],
    "contextType": "rare",
    "threat": "Potential Internal Recon",
    "threatDescription": "When a user who rarely interacts with a certain volume type then accesses it, this may represent suspicious activity.",
    "unit": "Anomaly Score",
    "unitDescription": "\"Anomaly Score\" represents how unusual it was for a user to interact with a specific volume type, when that user rarely uses that volume type. The anomaly is based on any use of a volume type by a user, compared to normal behavior.",
    "unitType": "Unknown",
    "bucketSize": "hourly"
  },
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.
- **rollupLevel** (required)
The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.
- **rollupId** (required)
The ID of the aggregate, alert or anomaly to match.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Responses

```
default
```

successful operation

GET `/search/{tid}/{entityType}`

Get entities of a specific type

Returns entities of the specified type sorted by `entityName`.

Example Response (Status 200)

```
{  
  "requestTime": 29,  
}
```



```

"data": [
  {
    "entityHash": "bc23443bd21342fa8997e",
    "entityType": "usr",
    "entityName": "Frank"
  },
  {
    "entityHash": "a89789b897e897d768ef8",
    "entityType": "usr",
    "entityName": "François"
  },
  {
    "entityHash": "9ba897e8978898e87fd76",
    "entityType": "usr",
    "entityName": "Joséphine"
  }
],
"totalHits": 25,
"scrollId": "vabsjk5h24e1kdasjfojdabhgjk32b5b",
"cached": false
}

```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **entityType** (required)
The entity type, for example, user, volume, printer, website, etc.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **count** (optional)
The number of entities to return.
- **sortOrder** (optional)

Specifies the sort order of the results. Possible values are desc and asc.

- **scrollId** (optional)

The scrollId from the previous request. Use this scrollId to get subsequent results.

Responses

default

successful operation

GET /search/{tid}/{entityType}/{entityHash}

Get entity details

Given an entity hash, returns the entity's name, type, bot score, tags and clusters.

```
{
  "requestTime": 29,
  "data": {
    "entityType": "user",
    "entityHash": "a1cb99f133d83b44",
    "entityName": "camilla",
    "botScore": 0.0007642867371433429,
    "tags": "[ BOT ]",
    "clusters": "[ KMEANS_2 ]"
  },
  "totalHits": 25,
  "scrollId": "vabsjk5h24e1kdasjfojdabhgjk32b5b",
  "cached": false
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **entityType** (required)
The entity type, for example, user, volume, printer, website, etc.
- **entityHash** (required)
Element hash (e.g., 393ff13c9b519ec2).

Request headers

- **Intersect-Version** (optional) -- String

Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Responses

default

successful operation

POST `/search/{tid}/entityByName`

Get entity details by entity name

Given an entity name and optionally an entity type, returns the entity's name, type, bot score, tags and clusters.

```
{
  "requestTime": 0,
  "data": {
    "entityType": "user",
    "entityHash": "c6b00f4cca9b3d9",
    "entityName": "jacquelyn.higdon",
    "botScore": 0.00032597667691905424,
    "tags": [],
    "clusters": [
      "KMEANS_5"
    ]
  },
  "cached": false
}
```

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request body

[ApiEntityNameRequest](#)

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Responses

default

successful operation

GET /search/{tid}/{entityType}/{entityHash}/risk

Get the entity risk score

Returns the current risk score for the specified entity for the specified time range. If the long format is requested, the entity's most significant alert is included in the response. The value of `riskChange` represents the change in risk over the past day. Note that the long format response and the risk change are populated only when the current risk score is requested for the entity.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "entityHash": "bc23443bd21342fa8997e",
    "entityType": "user",
    "entityName": "Annie",
    "risk": 25,
    "riskChange": -1,
    "lastActivity": 1453957200,
    "preDecayedRisk": 0,
    "decayedToTimestamp": 0,
    "mostSignificantAlert": {
      "id": "",
      "alertId": "",
      "datasource": "auth",
    }
  }
}
```

```

    "timestamp": 1459144000,
    "risk": 100,
    "contribution": 2,
    "significance": 100,
    "templates": {
      "threat": "",
      "family": "",
      "teaser": "",
      "alert": "",
      "tooltip": ""
    },
    "anomalyTypes": [],
    "numAnomalies": 3,
    "category": "Active Directory",
    "bucketSize": "hourly",
    "rollupLevel": "alerts",
    "numChildren": 3,
    "parentId": "aggId",
    "kibana": {
      "searchQuery": "",
      "indexName": ""
    },
    "contextAnomalyId": "",
    "contextType": "none"
  },
  "tags": [
    {
      "id": "9v3sdqdC2jd0FJCBuYcAPw",
      "name": "reviewed",
      "source": "user",
      "description": ""
    }
  ]
},
"cached": "false"
}

```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **entityType** (required)
The entity type, for example, user, volume, printer, website, etc.

- **entityHash** (required)
Element hash (e.g., 393ff13c9b519ec2).

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **sort** (optional)
The risk to return for the entity.
- **format** (optional)
The format of the response. When set to `long`, the top alert information for the entity is included in the response.
- **markup** (optional)
Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, `{{ and }}`. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.
- **tz** (optional)
The timezone in which the results should be returned (e.g., `+5:00, America/Montreal, EST`).
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

```
successful operation
```

GET /search/{tid}/{entityType}/{entityHash}/riskGraph

Get the entity risk graph

Returns a timeline of an entity's risk scores in a given time range. The risk returned in each time bucket represents the maximum risk for that entity within that bucket's time range.

Example Response (Status 200)

The first array represents the start of each time bucket in seconds. Buckets with no risk are omitted. Each item in the second array represents the risk score for the bucket at the same index in the first array.

```
{
  "requestTime": 29,
  "data": [
    {
      "risk": 14,
      "timestamp": 1457982000
    },
    {
      "risk": 5,
      "timestamp": 1458003600
    },
    {
      "risk": 12,
      "timestamp": 1458046800
    }
  ],
  "cached": "false"
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **entityType** (required)
The entity type, for example, user, volume, printer, website, etc.
- **entityHash** (required)
Element hash (e.g., 393ff13c9b519ec2).

Request headers

- **Intersect-Version** (optional) -- String

Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **count** (optional)

The number of time buckets to return between `ts` and `te`. Each time bucket contains the entity's maximum risk in that time range.

- **interval** (optional)

The bucket interval (supersedes the `count` parameter). Accepted values are: "day". Buckets are broken down based on the requested time zone.

- **tz** (optional)

The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

- **ts** (optional)

Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

- **te** (optional)

End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET /search/{tid}/users/bots

Get bot users

Returns bot users ordered by descending bot score.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "entityName": "anne@intserset.com",
      "entityHash": "aadfd74dc21710de",
      "entityType": "bot",
      "risk": 0.73,
      "tags": [
        {
          "id": "tagId0987",
          "name": "FORCEBOT",
          "source": "analytics",
          "description": ""
        },
        {
          "id": "tagId1244",
          "name": "BOT",
          "source": "analytics",
          "description": ""
        }
      ]
    }
  ],
  "cached": "false"
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Interset-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **count** (optional)
The number of bots to return

Responses

default

successful operation

GET /search/{tid}/distribution/risk

Get entity risk distribution

Returns the number of entities associated with each risk level at the most current time in the dataset.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "risks": {
      "high": 0,
      "total": 370,
      "low": 370,
      "medium": 0,
      "extreme": 0
    },
    "entityTypes": ["projects", "users"],
    "name": "risk",
    "count": 4,
    "type": "current"
  },
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.

- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **q** (optional)
Query filter.
- **includeAssociatedEntities** (optional)
If `false` and the `q` parameter filters for one or more entities and/or entity types, related entities of other entity types are not returned.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/{entityType}/distribution/risk

Get the entity risk distribution

Provides an overview of how many entities of the specified type are associated with each risk level at the most current time in the dataset.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "risks": {
      "high": 0,
      "total": 370,
      "low": 370,
      "medium": 0,
      "extreme": 0
    },
    "entityTypes": ["projects"],
    "name": "risk",
    "count": 4,
    "type": "current"
  },
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.
- **entityType** (required)
The entity type, for example, `user`, `volume`, `printer`, `website`, etc.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

`default`

successful operation

GET /search/{tid}/info

Get tenant data overview

Provides an overview of the tenant's data. Information includes scored entities and their counts, the total number of events analyzed, the anomalies discovered, and the time the tenant was last modified.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "timestart": 0,
    "timeend": 1488213317,
    "lastModified": 0,
    "totalDocs": 0,
    "totalScoredFiles": 0,
    "totalCurrentScoredFiles": 0,
    "totalScoredMachines": 0,
    "totalCurrentScoredMachines": 0,
    "totalScoredProjects": 0,
    "totalCurrentScoredProjects": 0,
    "totalScoredServers": 0,
    "totalCurrentScoredServers": 0,
    "totalScoredUsers": 0,
    "totalCurrentScoredUsers": 0,
    "totalScoredVolumes": 0,
    "totalCurrentScoredVolumes": 0,
    "totalScoredPrinters": 0,
    "totalCurrentScoredPrinters": 0,
    "totalScoredShares": 0,
    "totalCurrentScoredShares": 0,
    "totalScoredResources": 0,
    "totalCurrentScoredResources": 0,
    "totalScoredWebsites": 0,
    "totalCurrentScoredWebsites": 0,
    "totalScoredIps": 0,
    "totalCurrentScoredIps": 0,
    "totalAlerts": 0,
    "totalAnomalies": 0,
    "totalEvents": 0,
    "datasources": [
      "vpn",
      "auth",
      "netflow"
    ],
  },
}
```

```
"families": [],
"threatTypes": ["Suspicious Activity", "Potential Account Misuse"],
"uiMappings": {
  "volume": {
    "plural": "Volumes",
    "singular": "Volume",
    "query": "volume"
  },
  "server": {
    "plural": "Servers",
    "singular": "Server",
    "query": "server"
  },
  "website": {
    "plural": "Websites",
    "singular": "Website",
    "query": "website"
  },
  "file": {
    "plural": "Files",
    "singular": "File",
    "query": "file"
  },
  "resource": {
    "plural": "Resources",
    "singular": "Resource",
    "query": "resource"
  },
  "machine": {
    "plural": "Engines",
    "singular": "Engine",
    "query": "machine"
  },
  "ip": {
    "plural": "IP Addresses",
    "singular": "IP Address",
    "query": "ip"
  },
  "printer": {
    "plural": "Printers",
    "singular": "Printer",
    "query": "printer"
  },
  "project": {
    "plural": "Projects",
    "singular": "Project",
    "query": "project"
  },
  "share": {
    "plural": "Shares",
```

```

    "singular": "Share",
    "query": "share"
  },
  "user": {
    "plural": "Players",
    "singular": "Player",
    "query": "player"
  }
},
"features": [
  "awesomeFeature",
  "forAllFeature"
]
},
"cached": "false"
}

```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/matrix/{type}

Get anomaly matrix

Returns a grid representation of the number of anomalies for each risk and time range. Parameters `tn` and `rn` can be used to control the number of datapoints returned.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "id": "6e129a48-e3cb-471c-90a4-e431f53301e5",
    "query": null,
    "axis": {
      "type": "timestamp",
      "min": 1440388800,
      "max": 1445540400,
      "count": 10
    },
  },
  "dimensions": [
    {
      "maxvalue": 1640,
      "rows": 10,
      "axis": {
        "type": "risk",
        "min": 0,
        "max": 100,
        "count": 10
      },
    },
  ],
  "totalhits": 21745,
  "data": [
    [
      1475,
      1475,
      1514,
      1640,
      1227,
      1024,
      733,
```

```
    765,  
    782,  
    583  
  ],  
  [  
    305,  
    305,  
    338,  
    308,  
    244,  
    611,  
    255,  
    205,  
    496,  
    157  
  ],  
  [  
    25,  
    25,  
    127,  
    22,  
    20,  
    247,  
    94,  
    25,  
    125,  
    19  
  ],  
  [  
    500,  
    500,  
    408,  
    400,  
    400,  
    530,  
    400,  
    500,  
    579,  
    381  
  ],  
  [  
    0,  
    0,  
    51,  
    0,  
    0,  
    76,  
    0,  
    0,  
    0,
```

```
    0
  ],
  [
    0,
    0,
    12,
    0,
    0,
    0,
    0,
    0,
    0,
    0
  ],
  [
    50,
    50,
    40,
    40,
    40,
    116,
    40,
    50,
    50,
    38
  ],
  [
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0
  ],
  [
    50,
    50,
    37,
    40,
    40,
    40,
    40,
    50,
    50,
    38
  ],
],
```

```

    [
      100,
      100,
      80,
      80,
      80,
      92,
      80,
      100,
      100,
      76
    ]
  ]
}
]
},
"cached": "false"
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same entityType are automatically ORed, and those concerning different entities are ANDed.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **type** (required)
The type of anomaly representation that should be graphed on the matrix.

Request headers

- **Intersect-Version** (optional) -- String

Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **rn** (optional)
The number of risk rows to include in the matrix.
- **tn** (optional)
The number of time buckets into which the time window should be split (matrix columns)
- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET `/search/{tid}/riskGraph/breakdown`

Population risk breakdown

Returns a list of time buckets containing a breakdown of anomaly contribution to the population risk at each of those points in time. The risk can be included in the response by setting the query string parameter `includeRisk` to `true`. For performance reasons, we recommend that you call the `/riskGraph` endpoint if you are fetching only the risk.

A breakdown of contribution can be retrieved by:

- **risk:** Breakdown of anomaly risk levels that contributed to the current population risk
- **entityType:** Breakdown of the entityType involved in anomalies that contributed to the current population risk
- **threat/workingDays:** Breakdown of threat types involved in anomalies that contributed to the current population risk

Example Response (Status 200)

Example of population risk breakdown by entity type:

```
{
  "requestTime": 29,
  "data": {
    "breakdown": [
      {
        "timestamp": 1479898800,
        "timestampStr": "2016-11-23T03:00:00-08:00[America/Los_Angeles]",
        "groupBy": "entityType",
        "values": {
          "projects": {
            "contribution": 23.0
          },
          "servers": {
            "contribution": 37.0
          },
          "files": {
            "contribution": 15.0
          },
          "users": {
            "contribution": 25.0
          }
        }
      }
    ],
    "categories": [
      "files",
      "machines",
      "projects",
      "servers",
      "users",
      "volumes",
      "printers",
      "shares",
      "resources",
      "websites",
      "ips"
    ]
  }
},
```

```
"cached": "false"  
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **count** (optional)
If `interval` is set to `day`, the number of days to graph, working backwards from `te`; otherwise, the number of time buckets to return between `ts` and `te`. Each time bucket contains the entity's maximum risk in that time range. Maximum value of 100. The minimum bucket size is 1 hour.
- **interval** (optional)

Bucket interval (supersedes the count parameter). Accepted values are: "day". Buckets are broken down based on the requested timezone.

- **breakdownBy** (optional)
Specifies how the risk contribution is broken down
- **includeRisk** (optional)
When true, indicates that the risk for each bucket should be returned. The risk can be retrieved in parallel for the same buckets by using the /riskGraph endpoint with the same parameters.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET /search/{tid}/riskGraph

Population risk graph

Returns a list of time buckets containing the population risk at each of those points in time. The risk in each bucket represents a combination of the risk scores at that time for each entity not filtered out.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "breakdown": [
      {
        "timestamp": 1479898800,
        "timestampStr": "2016-11-23T03:00:00-08:00[America/Los_Angeles]",
        "risk": 32.0
      },
      {
        "timestamp": 1479985200,
        "timestampStr": "2016-11-24T03:00:00-08:00[America/Los_Angeles]",
        "risk": 38.0
      }
    ]
  },
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same entityType are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **count** (optional)
Number of time buckets to return between `ts` and `te`. Each time bucket will contain the entity's maximum risk in that time range.
- **interval** (optional)
Bucket interval (will supersede `count` parameter). Accepted values are: "day". Buckets will be broken down based on the requested timezone.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/riskyHours

Get risky hours

Returns a list of hours during which the specified entity had anomalies. Each hour is accompanied by the maximum risk of the entity at that time.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "hour": 1357920900,
      "significance": 100.0
    },
    {
      "hour": 1357920900,
      "significance": 99.0
    },
    {
      "hour": 1357920900,
      "significance": 98.01
    },
    {
      "hour": 1357920900,
      "significance": 37.89
    }
  ],
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **minRisk** (optional)
Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.
- **maxRisk** (optional)
Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.
- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/templates

Get examples of rendered alert templates

Returns an example showing how each anomaly type is rendered into a human-readable sentence using the templating engine. The response can be filtered to retrieve only anomalies of a single type or belonging to a specific datasource.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "template": {
        "threat": "Suspicious Activity",
        "family": "Application/Protocol Use",
        "teaser": "7-8 PM Dec 20, 2012: Used EXPLORER rare for User.",
        "alert": "It was very unusual that {user1} used the application EXPLORER,
having only used that application 2 days.",
        "tooltip": ""
      },
      "category": "Endpoint",
      "threat": {
        "name": "Suspicious Activity",
        "description": "When a user who rarely uses an application then uses it, this
may represent suspicious activity."
      },
      "family": {
        "name": "Application/Protocol Use"
      },
      "anomalyType": 129,
      "datasource": "endpoint"
    }
  ],
  "cached": "false"
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **ds** (optional)
Data source
- **anomalyType** (optional)
Anomaly type
- **markup** (optional)
Indicates whether to include handlebar markup in alert text. When false, the returned anomalies contain only plain English text that can be displayed directly without further processing. When true, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.

Responses

default

successful operation

GET /search/{tid}/{entityType}/topAccessed

Get the top accessed entities by entity type

Returns a list of entities, ordered by the number of times they were accessed.

Example Response (Status 200)

The keys represent the number of accesses, and their respective values represent the entities that recorded that number of accesses

```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "server1"
      },
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "server",
        "entityName": "server2"
      }
    ],
    "8": [
      {
        "entityHash": "64d7794788a116f964733",
        "entityType": "server",
        "entityName": "server3"
      }
    ],
    "4": [
      {
        "entityHash": "af867786e09453b67457c",
        "entityType": "server",
        "entityName": "server4"
      }
    ]
  },
  "cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid:** Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user:** Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.

- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.
- **entityType** (required)
The entity type, for example, user, volume, printer, website, etc.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **count** (optional)
The number of top accessed entities to return
- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/users/topExitProducers

Get top producers of exit events

Returns the users with the top number of events representing information exiting the system, for example, through a printer or USB.

Example Response (Status 200)

The keys represent the number of exit events, and their respective values represent the entities that generated that number of exit events.

```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "elavigne@interset.com"
      },
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "server",
        "entityName": "rwall@interset.com"
      }
    ],
    "8": [
      {
        "entityHash": "64d7794788a116f964733",
        "entityType": "server",
        "entityName": "mcyze@interset.com"
      }
    ],
    "4": [
      {
        "entityHash": "af867786e09453b67457c",
        "entityType": "server",
        "entityName": "jmahonin@interset.com"
      }
    ]
  }
}
```

```

    ]
  },
  "cached": "false"
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators `AND` and `OR` serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically `ORed`, and those concerning different entities are `ANDed`.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Interset-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **count** (optional)
The number of top exit producers to return
- **q** (optional)
Query filter.

- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/users/topFailedLogin

Get top failed logins

Returns the users with the top number of failed login attempts.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "elavigne@interset.com",
      "entityName": "bc23443bd21342fa8997e",
      "totalSuccess": 25,
      "totalFailed": 33
    },
    {
      "entityHash": "rwall@interset.com",
      "entityName": "a89789b897e897d768ef8",
      "totalSuccess": 35,
      "totalFailed": 17
    },
    {
      "entityHash": "mcyze@interset.com",
      "entityName": "64d7794788a116f964733",
      "totalSuccess": 18,
      "totalFailed": 13
    }
  ]
}
```

```
],
"cached": "false"
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same entityType are automatically ORed, and those concerning different entities are ANDed.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **count** (optional)
The number of top users with failed logins to return
- **q** (optional)
Query filter.

- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/users/topScreenCaptures

Get top producers of screen captures

Returns the users with the top number of screen captures within the specified time period.

Example Response (Status 200)

The keys represent the number of screen captures, and their respective values represent the entities that generated that number of screen captures.

```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "elavigne@interset.com"
      },
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "server",
        "entityName": "rwall@interset.com"
      }
    ],
    "8": [
      {
        "entityHash": "64d7794788a116f964733",
```

```

        "entityType": "server",
        "entityName": "mcyze@interset.com"
    }
  ],
  "4": [
    {
      "entityHash": "af867786e09453b67457c",
      "entityType": "server",
      "entityName": "jmahonin@interset.com"
    }
  ]
},
"cached": "false"
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators `AND` and `OR` serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically `ORed`, and those concerning different entities are `ANDed`.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Interset-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call `GET /api/info/build` to see available API versions.

Query parameters

- **count** (optional)
The number of users to return.
- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/users/topViolationProducers

Get top violation producers

Returns the users that triggered the most violations within the specified time period.

Example Response (Status 200)

The keys represent the number of violation events, and their respective values represent the entities that generated that number of violations.

```
{
  "requestTime": 29,
  "data": {
    "12": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "server",
        "entityName": "elavigne@interset.com"
      }
    ],
  },
}
```

```

    {
      "entityHash": "a89789b897e897d768ef8",
      "entityType": "server",
      "entityName": "rwall@interset.com"
    }
  ],
  "8": [
    {
      "entityHash": "64d7794788a116f964733",
      "entityType": "server",
      "entityName": "mcyze@interset.com"
    }
  ],
  "4": [
    {
      "entityHash": "af867786e09453b67457c",
      "entityType": "server",
      "entityName": "jmahonin@interset.com"
    }
  ]
},
"cached": "false"
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same entityType are automatically ORed, and those concerning different entities are ANDed.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **count** (optional)
The number of top violation producers to return.
- **q** (optional)
Query filter.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET `/search/{tid}/typeAhead`

Auto-complete entity name for any entity type

Returns entities across all entity types that have part of their name starting with the value provided in the text parameter.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "users": [
      {
        "entityHash": "bc23443bd21342fa8997e",
        "entityType": "user",
        "entityName": "user1",
        "risk": 100,
        "riskChange": 0,
        "lastActivity": 1453957200,
        "preDecayedRisk": 0,
        "decayedToTimestamp": 0,
        "mostSignificantAlert": null,
        "tags": []
      }
    ],
    "files": [
      {
        "entityHash": "a89789b897e897d768ef8",
        "entityType": "file",
        "entityName": "u-some-file",
        "risk": 100,
        "riskChange": 0,
        "lastActivity": 1453957200,
        "preDecayedRisk": 0,
        "decayedToTimestamp": 0,
        "mostSignificantAlert": null,
        "tags": []
      }
    ]
  },
  "cached": "false"
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **count** (optional)
The max number of entities to return per entity type
- **text** (required)
The text to be used to match entity(ies) by name.
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET `/search/{tid}/users/{userHash}/workingHours/daily`

Get daily working hours per user

Returns an array of expected activity for the specified user for each half hour of the day. The minute represents the beginning of the half hour period, and the expected value represents the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 0,
      "expected": 0.6
    },
    {
      "minute": 30,
      "expected": 0.78
    },
    {
      "minute": 60,
      "expected": 0.87
    },
    {
      "minute": 90,
      "expected": 0.9
    },
    {
      "minute": 120,
      "expected": 1.1
    }
  ],
  "cached": "false"
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **userHash** (required)
Element hash for a user entity (e.g., 393ff13c9b519ec2).

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

GET /search/{tid}/users/workingHours/weekly

Get weekly working hours for the organization

Returns an array of expected activity for the entire organization for each half hour of the week. The minute represents the beginning of the half hour period, and the expected value represents the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 150,
      "expected": 1.1
    },
    {
      "minute": 180,
      "expected": 1.2
    },
    {
      "minute": 210,
      "expected": 0.9
    },
    {
      "minute": 240,
      "expected": 0.5
    },
    {
      "minute": 270,
      "expected": 0.0
    }
  ],
  "cached": "false"
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

GET /search/{tid}/users/workingHours/daily

Get daily working hours for the organization

Returns an array of expected activity for the entire organization for each half hour of the day. The minute represents the beginning of the half hour period, and the expected value represents the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 0,
      "expected": 0.6
    },
    {
      "minute": 30,
      "expected": 0.78
    }
  ]
}
```

```

    },
    {
      "minute": 60,
      "expected": 0.87
    },
    {
      "minute": 90,
      "expected": 0.9
    },
    {
      "minute": 120,
      "expected": 1.1
    }
  ],
  "cached": "false"
}

```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

GET /search/{tid}/users/{userHash}/workingHours/weekly

Get weekly working hours per user

Returns an array of expected activity for the specified user for each half hour of the week. The minute represents the beginning of the half hour period, and the expected value represents

the level of activity expected for that half hour period. The expected values form a histogram and are not normalized to a particular scale.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "minute": 150,
      "expected": 1.1
    },
    {
      "minute": 180,
      "expected": 1.2
    },
    {
      "minute": 210,
      "expected": 0.9
    },
    {
      "minute": 240,
      "expected": 0.5
    },
    {
      "minute": 270,
      "expected": 0.0
    }
  ],
  "cached": "false"
}
```

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **userHash** (required)
Element hash for a user entity (e.g., 393ff13c9b519ec2).

Request headers

- **Intersect-Version** (optional) -- String

Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Responses

default

successful operation

GET /search/{tid}/topRisky

Get top risky entities

Returns a list of all top risky entities.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "bc23443bd21342fa8997e",
      "entityType": "user",
      "entityName": "Annie",
      "risk": 25,
      "riskChange": 0,
      "lastActivity": 1453957200,
      "preDecayedRisk": 0,
      "decayedToTimestamp": 0,
      "mostSignificantAlert": null,
      "tags": [
        {
          "id": "9v3sdqdC2jd0FJCBuYcAPw",
          "name": "reviewed",
          "source": "user",
          "description": ""
        }
      ]
    }
  ],
  "totalHits": 25,
  "scrollId": "vabsjk5h24e1kdasjfojdabhgjk32b5b",
}
```

```
"cached": false  
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **sort** (optional)
Risk sort order in which to return entities.
- **format** (optional)
The format of the response. When set to `long`, the top alert information for the entity is included in the response.

- **q** (optional)
Query filter.
- **includeAssociatedEntities** (optional)
If `false` and the `q` parameter filters for one or more entities and/or entity types, related entities of other entity types are not returned.
- **markup** (optional)
Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, `{{ and }}`. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.
- **tz** (optional)
The timezone in which the results should be returned (e.g., `+5:00, America/Montreal, EST`).
- **count** (optional)
Number of top risky entities to return
- **scrollId** (optional)
The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.
- **includeNonAnomalous** (optional)
Set to `true` to include entities that never triggered anomalies
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

```
default
```

successful operation

GET /search/{tid}/{entityType}/topRisky

Get top risky entities by type

Returns a list of the top riskiest entities by type.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "bc23443bd21342fa8997e",
      "entityType": "user",
      "entityName": "Annie",
      "risk": 25,
      "riskChange": 0,
      "lastActivity": 1453957200,
      "preDecayedRisk": 0,
      "decayedToTimestamp": 0,
      "mostSignificantAlert": null,
      "tags": [
        {
          "id": "9v3sdqdC2jd0FJCBuYcAPw",
          "name": "reviewed",
          "source": "user",
          "description": ""
        }
      ]
    }
  ],
  "totalHits": 25,
  "scrollId": "vabsjk5h24e1kdasjfojdabhgjk32b5b",
  "cached": false
}
```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same entityType are automatically ORed, and those concerning different entities are ANDed.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **entityType** (required)
The entity type, for example, user, volume, printer, website, etc.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **sort** (optional)
Risk sort order in which to return entities.
- **format** (optional)
The format of the response. When set to long, the top alert information for the entity is included in the response.
- **q** (optional)
Query filter.
- **markup** (optional)
Indicates whether to include handlebar markup in alert text. When false, the returned anomalies contain only plain English text that can be displayed directly without further processing. When true, anomalies may contain markup tags in double curly braces, {{ and }}. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.
- **tz** (optional)
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).
- **count** (optional)
The number of top risky entities to return
- **scrollId** (optional)

The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

- **includeNonAnomalous** (optional)
Set to true to include entities that never triggered anomalies
- **ts** (optional)
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te** (optional)
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.

Responses

default

successful operation

GET /search/{tid}/{rollupLevel}/{rollupId}/expand

Get children of aggregate/alert/anomaly

Returns the children of the specified rollup ID. If an aggregate ID is specified, this method returns the child alerts. If an alert ID is specified, the child anomalies are returned. Nothing is returned when an anomaly ID is specified because anomalies are the lowest level and have no children.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "id": "ebea3079901fd4c1",
      "alertId": "ebea3079901fd4c1",
      "datasource": "repo",
      "timestamp": 1393453400,
      "risk": 8100,
      "contribution": 100,
      "significance": 88,
      "templates": {
        "threat": "",

```

```

    "family": "",
    "teaser": "",
    "alert": "",
    "tooltip": ""
  },
  "anomalyTypes": [
    11
  ],
  "numAnomalies": 2,
  "category": "Repository",
  "bucketSize": "hourly",
  "rollupLevel": "alerts",
  "numChildren": 2,
  "parentId": null,
  "kibana": {
    "searchQuery": "",
    "indexName": ""
  },
  "contextAnomalyId": "",
  "contextType": "none"
}
],
"totalHits": 25,
"cached": false,
"scrollId": "vabsjk5h24e1kdasjfojdabhgjk32b5b"
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the entityHash; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the entityName; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same entityType are automatically ORed, and those concerning different entities are ANDed.

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **rollupLevel** (required)
The level at which anomalies are combined. Aggregates combine similar alerts within the same time period across entities. Alerts combine similar anomalies within the same time period for a single entity.
- **rollupId** (required)
The ID of the aggregate, alert or anomaly to match.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **minRisk** (optional)
Minimum anomaly/alert risk. All anomalies/alerts below this threshold are excluded from the results.
- **maxRisk** (optional)
Maximum anomaly/alert risk. All anomalies/alerts above this threshold are excluded from the results.
- **count** (optional)
- **q** (optional)
Query filter.
- **markup** (optional)
Indicates whether to include handlebar markup in alert text. When `false`, the returned anomalies contain only plain English text that can be displayed directly without further processing. When `true`, anomalies may contain markup tags in double curly braces, `{{` and `}}`. For more information about rendering the returned anomalies, see the Introduction section of the developer guide.
- **scrollId** (optional)
The `scrollId` from the previous request. Use this `scrollId` to get subsequent results.

- **sort** (optional)
Method of sorting alerts.
- **sortOrder** (optional)
Specifies the sort order of the results. Possible values are desc and asc.
- **riskSort** (optional)
Risk sort order in which to return entities.
- **scType** (optional)
Scaled contribution. Deprecated; use minRisk.
- **sc** (optional)
Scaled contribution. Deprecated; use minRisk.

Responses

default

successful operation

search{tenantId}meta

POST /search/{tid}/meta

Create a meta resource

Creates a new meta resource. Fields that must be added: resourceType, destinationId, destinationType, content, contentType

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data":
  {
    "id": "cb3c32ebc26d8463",
    "resourceType": "annotation",
    "sourceId": "abc@interset.com",
    "sourceType": "user",
    "destinationId": "b2d1bbfd2daa1fed",
    "destinationType": "entities",
    "content": "",
    "contentType": "html",
  }
}
```

```
"createdBy": "abc@interset.com"  
"created": 1541603226  
"timestamp": 1541725744  
},  
"cached": "false"  
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request body

[ApiMetaRequest](#)

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

DELETE /search/{tid}/meta/{metaId}

Delete a meta resource

Deletes the meta resource with the specified ID.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "Meta resource with ID 6f327e088def9386 successfully deleted."
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **metaId** (required)
The ID of the meta resource (e.g., cb3c32ebc26d8463).

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

GET /search/{tid}/meta/log

Get all meta logs for a tenant with certain conditions.

Get all meta logs for this tenant with the search conditions specified. Source type can be configured either by a user through the UI, or by Analytics. Currently supported destination types are alerts, anomalies and entities

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "id": "423c32ebc26d8bce",
      "resourceId": "null",
      "resourceType": "comment",
      "action": "create",
      "sourceId": "def@interset.com",
      "sourceType": "user",
      "destinationId": "8202835f7614404d",
      "destinationType": "alerts",
      "content": "This is my very first comment.",
      "contentType": "plaintext",
      "created": 1541603226
      "createdBy": "def@interset.com"
      "modifiedBy": null
      "timestamp": 1541603226
    },
    {
      "id": "cb3c32ebc26d8463",
      "resourceId": "423c32ebc26d8bce",
      "resourceType": "comment",
      "action": "update",
      "sourceId": "abc@interset.com",
      "sourceType": "user",
      "destinationId": "b2d1bbfd2daa1fed",
      "destinationType": "entities",
      "content": "This is my very first *edited* comment.",
      "contentType": "markdown",
      "created": 1541603226
      "createdBy": "abc@interset.com"
      "modifiedBy": "admin@interset.com"
      "timestamp": 1541725744
    },
  ],
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **q** (optional)
Query filter.
- **resourceId** (optional)
A reference to the original resource if applicable (metaId, tagId, null)
- **resourceType** (optional)
The type of the meta resource e.g. comment, annotation, tag, dashboard, visualization and so on.
- **action** (optional)
The operation made on this meta resources. This API supports add, update, delete.
- **sourceId** (optional)
The ID of the source. If the source type is user, then createdBy is the user's name.
- **sourceType** (optional)
The type of the source. Currently supported: user, analytics
- **destinationId** (optional)
The ID of the destination.
- **destinationType** (optional)
The type of the source. Currently supported: alerts, anomalies, entities
- **content** (optional)
The raw content of the object. This is a full text search. Larger than 128KB can significantly impact the search performance.

- **contentType** (optional)
Currently supported: markdown, plaintext, html
- **createdBy** (optional)
The name of the user that original created the resource - an informational field.
- **modifiedBy** (optional)
The ID of the user that last modified the resource.

Responses

default

successful operation

GET /search/{tid}/meta/{metaId}

Get the specified meta resource.

Gets the meta resource with the specified ID.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data":
  {
    "id": "cb3c32ebc26d8463",
    "resourceType": "annotation",
    "action": "update",
    "sourceId": "abc@interset.com",
    "sourceType": "user",
    "destinationId": "b2d1bbfd2daa1fed",
    "destinationType": "entities",
    "content": "",
    "contentType": "html",
    "created": 1541603226
    "createdBy": "abc@interset.com"
    "modifiedBy": "admin@interset.com"
    "timestamp": 1541725744
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **metaId** (required)
The ID of the meta resource (e.g., cb3c32ebc26d8463).

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

GET /search/{tid}/meta

Get all meta resources for a tenant with certain conditions.

Get all meta resources for this tenant with the search conditions specified. Source type can be configured either by a user through the UI, or by Analytics. Currently supported destination types are alerts, anomalies and entities

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
```

```

    "id": "423c32ebc26d8bce",
    "resourceId": "null",
    "resourceType": "comment",
    "action": "create",
    "sourceId": "def@interset.com",
    "sourceType": "user",
    "destinationId": "8202835f7614404d",
    "destinationType": "alerts",
    "content": "This is my very first comment.",
    "contentType": "plaintext",
    "created": 1541603226
    "createdBy": "def@interset.com"
    "modifiedBy": null
    "timestamp": 1541603226
  },
  {
    "id": "cb3c32ebc26d8463",
    "resourceId": "423c32ebc26d8bce",
    "resourceType": "comment",
    "action": "update",
    "sourceId": "abc@interset.com",
    "sourceType": "user",
    "destinationId": "b2d1bbfd2daa1fed",
    "destinationType": "entities",
    "content": "This is my very first *edited* comment.",
    "contentType": "markdown",
    "created": 1541603226
    "createdBy": "abc@interset.com"
    "modifiedBy": "admin@interset.com"
    "timestamp": 1541725744
  },
],
"cached": "false"
}

```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **q** (optional)
Query filter.
- **resourceType** (optional)
The type of the meta resource e.g. comment, annotation, tag, dashboard, visualization and so on.
- **action** (optional)
The operation made on this meta resources. This API supports add, update, delete.
- **sourceId** (optional)
The ID of the source. If the source type is user, then createdBy is the user's name.
- **sourceType** (optional)
The type of the source. Currently supported: user, analytics
- **destinationId** (optional)
The ID of the destination.
- **destinationType** (optional)
The type of the source. Currently supported: alerts, anomalies, entities
- **content** (optional)
The raw content of the object. This is a full text search. Larger than 128KB can significantly impact the search performance.
- **contentType** (optional)
Currently supported: markdown, plaintext, html
- **createdBy** (optional)
The name of the user that original created the resource - an informational field.
- **modifiedBy** (optional)
The ID of the user that last modified the resource.

Responses

default

successful operation

PUT /search/{tid}/meta/{metaId}

Update a meta resource

Update the specified a meta resource. Fields that can be updated: resourceType, destinationId, destinationType, content, contentType

Example Response (Status 200)

```
{
  "resourceType": "annotation",
  "id": "cb3c32ebc26d8463",
  "sourceId": "abc@interset.com",
  "sourceType": "user",
  "destinationId": "b2d1bbfd2daa1fed",
  "destinationType": "entities",
  "content": "",
  "contentType": "html",
  "createdBy": "abc@interset.com"
  "modifiedBy": "admin@interset.com"
  "created": 1541603226
  "timestamp": 1541725744
},
"cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **metaId** (required)
The ID of the meta resource (e.g., cb3c32ebc26d8463).

Request body

[ApiMetaRequest](#)

Changes the resource type, source, destination, content and modifiedBy for the specified meta resource.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

search{tenantId}tags

PUT /search/{tid}/tags/{tagId}/{tagElementType}/{elementHash}

Add a tag to an element

Adds a tag to an element such as an entity or an alert.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully associated with 'entities' element
75c2599ddf50ea85"
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).
- **elementHash** (required)
Element hash (e.g., 393ff13c9b519ec2).
- **tagElementType** (required)
The type of element with which the tag is associated.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **retries** (optional)
The number of times to retry the update operation if a conflict occurs.

Responses

default

successful operation

POST /search/{tid}/tags/{tagId}/{tagElementType}/add

Add a tag to multiple elements

Adds a tag to a list of elements of the same type.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully associated with entities:
["75c2599ddf50ea85", "75c2599ddf50ea86]"
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).
- **tagElementType** (required)
The type of element with which the tag is associated.

Request body

[ApiTagEntities](#)

A list of element hashes.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **retries** (optional)

The number of times to retry the update operation if a conflict occurs.

Responses

default

successful operation

POST /search/{tid}/tags

Create a tag

Creates a new tag.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "name": "newTag",
    "description": "testing tags",
    "entities": [],
    "id": "6f327e088def9386",
    "created": "2017-12-01T00:16:56.016Z",
    "createdBy": "td5",
    "modified": "2017-12-01T00:16:56.016Z",
    "modifiedBy": "td5",
    "source": "user"
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.

Request body

[TagBase](#)

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Responses

default

successful operation

DELETE /search/{tid}/tags/{tagId}

Delete a tag

Deletes the tag with the specified ID.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "Tag 6f327e088def9386 successfully deleted."
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **force** (optional)
Force the action to be applied even in the presence of conflicts.

Responses

default

successful operation

GET /search/{tid}/tags/{tagId}/{tagElementType}

Get elements associated with a particular tag

Gets all elements that have the specified tag.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "e6a4bb7b21cf495b",

```



```

    "entityType": "user",
    "entityName": "user1041@dev-win-10-conn"
  }
],
"cached": "false"
}

```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).
- **tagElementType** (required)
The type of element with which the tag is associated.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **count** (optional)
The number of tagged elements to return.
- **scrollId** (optional)
The scrollId from the previous request. Use this scrollId to get subsequent results.

Responses

default

successful operation

GET /search/{tid}/tags/{tagId}

Get the specified tag

Gets the tag with the specified ID.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "name": "recon",
    "description": null,
    "entities": [],
    "id": "46b489f7f46588c6",
    "created": "2017-11-30T23:59:38.737Z",
    "createdBy": "td5",
    "modified": "2017-12-01T00:16:56.016Z",
    "modifiedBy": "td5",
    "source": "user"
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Responses

default

successful operation

GET /search/{tid}/tags/{boolOperator}/entities

Get elements associated with tags

Returns entities that match the specified tags.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "entityHash": "75c2599ddf50ea85",
      "entityType": "user",
      "entityName": "user68@qa-win-7-conn.local"
    }
  ],
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **boolOperator** (required)
Indicates whether the returned entities must have any or all of the specified tags. Possible values are any (return entities with any of the specified tags) or all (return entities with all the specified tags).

Request headers

- **Intersect-Version** (optional) -- String

Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **tag** (optional)
A list of tags, formatted as tag=<tagID1>&tag=<tagID2>&tag=<tagID3> In the UI, enter unquoted tag IDs in the textbox, one per line.
- **count** (optional)
The number of tagged elements to return.
- **scrollId** (optional)
The scrollId from the previous request. Use this scrollId to get subsequent results.

Responses

default

successful operation

GET /search/{tid}/tags

Get all tags for a tenant

Get all tags for this tenant. Tags can be configured either by a user through the UI, or by Analytics. The payload specifies the source of the tag.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": [
    {
      "name": "exfiltrate",
      "description": null,
      "entities": [],
      "id": "f2c23b9def498aeb",
      "created": "2017-11-30T23:58:55.529Z",
      "createdBy": "td5",
```

```

    "modified": "2017-12-01T00:16:56.016Z",
    "modifiedBy": "td5",
    "source": "user"
  },
  {
    "name": "recon",
    "description": null,
    "entities": [],
    "id": "46b489f7f46588c6",
    "created": "2017-11-30T23:59:38.737Z",
    "createdBy": "td5",
    "source": "user"
  }
],
"cached": "false"
}

```

Filtering the results

The results can be filtered using the `q` parameter, which accepts a filter query (e.g., `userid:a1cb99f133d83b44 AND risk:extreme`):

- **userid**: Allows filtering using the `entityHash`; use `serverid`, `projectid`, and so on, to filter on other types of scored entities.
- **user**: Allows filtering using the `entityName`; use `server`, `project`, and so on, to filter on other types of scored entities.
- **risk**: Allows filtering by risk level (low, medium, high, extreme).
- **anomalies**: Allows filtering by anomaly types (e.g., `anomalies:201,202`).

Although the operators AND and OR serve as separators between different filters, their respective values are currently ignored. Filters concerning the same `entityType` are automatically ORed, and those concerning different entities are ANDed.

Consumes

- `application/json`

Produces

- `application/json`

Path parameters

- **tid** (required)
The tenant ID.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Query parameters

- **source** (optional)
Indicates how the tag was created (either by a user or by analytics).
- **q** (optional)
Query filter.
- **typeahead** (optional)
The text to be used to match tags by name.

Responses

```
default
```

successful operation

DELETE `/search/{tid}/tags/{tagId}/{tagElementType}/ {elementHash}`

Remove a tag from a single element

Deletes a tag from an element such as an entity or an alert.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully removed from 'entities' element
75c2599ddf50ea85"
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).
- **elementHash** (required)
The element hash (e.g., 393ff13c9b519ec2).
- **tagElementType** (required)
The type of element with which the tag is associated.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **retries** (optional)
The number of times to retry the update operation if a conflict occurs.

Responses

default

successful operation

POST /search/{tid}/tags/{tagId}/{tagElementType}/remove

Remove a tag from multiple elements

Deletes a tag from a list of elements of the same type.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "message": "46b489f7f46588c6 successfully removed from entities:
["75c2599ddf50ea85", "75c2599ddf50ea86"]"
  }, "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).
- **tagElementType** (required)
The type of element with which the tag is associated.

Request body

[ApiTagEntities](#)

A list of element hashes.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Query parameters

- **retries** (optional)

The number of times to retry the update operation if a conflict occurs.

Responses

default

successful operation

POST /search/{tid}/tags/{tagId}/update

Update a tag

Changes the specified a tag.

Example Response (Status 200)

```
{
  "requestTime": 29,
  "data": {
    "name": "changedTag",
    "description": "testing tags",
    "entities": [],
    "id": "6f327e088def9386",
    "created": "2017-12-01T00:16:56.016Z",
    "createdBy": "td5",
    "modified": "2017-12-01T00:16:56.016Z",
    "modifiedBy": "td5",
    "source": "user"
  },
  "cached": "false"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
The tenant ID.
- **tagId** (required)
The ID of the tag (e.g., mQhWWuPFNqti-w-AINWHdA).

Request body

TagBase

Changes the name, description, and the list of entity hashes for the specified tag.

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET `/api/info/build` to see available API versions.

Responses

default

successful operation

tenants

DELETE /tenants/{tid}

Delete a tenant

Delete the specified tenant.

Produces

- application/json

Path parameters

- **tid** (required)

Responses

default

successful operation

DELETE /tenants/{tid}/users/{userId}

Delete a user

Delete the specified user from the specified tenant. Permissions and sessions for the user are also deleted. If the user exists in another tenant, that user is not deleted.

Produces

- application/json

Path parameters

- **tid** (required)
- **userId** (required)

Responses

default

successful operation

GET /tenants/{tid}

Get tenant details

Get details for the specified tenant.

Produces

- application/json

Path parameters

- **tid** (required)

Return type

[Tenant](#)

Example data

Content-Type: application/json

```
{
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interaset"
}
```

Responses

200

successful operation

GET /tenants/{tid}/users

Get list of users for tenant

Get the list of users for the specified tenant.

Produces

- application/json

Path parameters

- **tid** (required)

Return type

array[[ApiTenantUser](#)]

Example data

Content-Type: application/json

```
[ {
  "persistentSessions" : false,
```

```

    "password" : "password123",
    "role" : "admin",
    "permissions" : "[\"ACCESS_INTELLIGENCE\", \"VIEW_INTELLIGENCE_RAW_
EVENTS\"]",
    "created" : 0,
    "tenantId" : "0",
    "name" : "Camilla Ferguson",
    "isActive" : true,
    "userId" : "camilla",
    "local" : false
  }, {
    "persistentSessions" : false,
    "password" : "password123",
    "role" : "admin",
    "permissions" : "[\"ACCESS_INTELLIGENCE\", \"VIEW_INTELLIGENCE_RAW_
EVENTS\"]",
    "created" : 0,
    "tenantId" : "0",
    "name" : "Camilla Ferguson",
    "isActive" : true,
    "userId" : "camilla",
    "local" : false
  } ]

```

Responses

200

successful operation

GET /tenants

Get the list of tenants

Get the list of all tenants.

Produces

- application/json

Return type

array[Tenant]

Example data

Content-Type: application/json

```
[ {
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interaset"
}, {
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interaset"
} ]
```

Responses

200

successful operation

GET /tenants/{tid}/users/{userId}

Get user details for a tenant

Get details about the specified user for the specified tenant.

Produces

- application/json

Path parameters

- **tid** (required)
- **userId** (required)

Return type

[ApiTenantUser](#)

Example data

Content-Type: application/json

```
{
  "persistentSessions" : false,
  "password" : "password123",
  "role" : "admin",
  "permissions" : "[\\"ACCESS_INTELLIGENCE\\",\\"VIEW_INTELLIGENCE_RAW_
EVENTS\\"]",
  "created" : 0,
  "tenantId" : "0",
  "name" : "Camilla Ferguson",
  "isActive" : true,
  "userId" : "camilla",
  "local" : false
}
```

Responses

200

successful operation

PUT /tenants/{tid}

Update tenant details

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)

Request body

[Tenant](#)

Return type

[Tenant](#)

Example data

Content-Type: application/json

```
{
  "created" : "2000-01-23T04:56:07.000+00:00",
  "tenantId" : "a3b",
  "name" : "Interaset"
}
```

Responses

200

successful operation

PUT /tenants

Set details for multiple tenants

Consumes

- application/json

Request body

[array\[Tenant\]](#)

Responses

default

successful operation

PUT /tenants/{tid}/users/{userId}

Update user details

Create or update the details of a user, or link a user to a tenant.

When you link an existing user to a tenant, the body of the request must contain only the role, userId and tenantId fields. Any update to the name and password fields must be made

against a tenant with which the user is already associated, unless it is a new user, in which case it can be created and linked to a tenant in the same request.

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)
- **userId** (required)

Request body

[ApiTenantUser](#)

Request headers

- **Intersect-Version** (optional) -- String
Indicates which version of the API to use. Defaults to the latest version. Call GET /api/info/build to see available API versions.

Return type

[ApiTenantUser](#)

Example data

Content-Type: application/json

```
{
  "persistentSessions" : false,
  "password" : "password123",
  "role" : "admin",
  "permissions" : "[\\"ACCESS_INTELLIGENCE\\",\\"VIEW_INTELLIGENCE_RAW_EVENTS\\"]",
  "created" : 0,
  "tenantId" : "0",
  "name" : "Camilla Ferguson",
```

```
"isActive" : true,  
"userId" : "camilla",  
"local" : false  
}
```

Responses

200

successful operation

theme

DELETE /theme/{tid}

Delete a custom theme

Produces

- application/json

Path parameters

- **tid** (required)

Responses

default

successful operation

DELETE /theme

Delete a default theme

Produces

- application/json

Responses

default

successful operation

GET /theme

Get default theme

Returns a map of the default theme information, or {} if none is set. You can set one default theme for your cluster.

Themes change the look and feel of applications by altering colors, text labels, and images.

Example Response (Status 200)

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

Produces

- application/json

Responses

default

successful operation

GET /theme/{tid}

Get a custom theme

Returns a map of the custom theme information for the specified tenant, or {} if none is set.

Themes change the look and feel of applications by altering colors, text labels, and images.

Example Response (Status 200)

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

Produces

- application/json

Path parameters

- **tid** (required)

Responses

default

successful operation

PUT /theme*Update default theme*

Sets the default theme. You can set one default theme for your cluster.

Themes change the look and feel of applications by altering colors, text labels, and images.

Example Request Body

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

Consumes

- application/json

Produces

- application/json

Request body

[ApiTheme](#)

Responses

default

successful operation

PUT /theme/{tid}

Update a custom theme

Sets the custom theme for the specified tenant.

Themes change the look and feel of applications by altering colors, text labels, and images.

Example Request Body

```
{
  "loginGradient1": "linear-gradient(#b4bbc6 65%, #737b83)",
  "loginGradient2": "linear-gradient(#eda24e 65%, #e56443)",
  "accent": "#333333",
  "navBar": "rgb(68, 68, 68)",
  "font1": "hsl(0, 0%, 33%)",
  "font2": "hsl(0, 0%, 40%)",
  "font3": "hsl(0, 0%, 67%)",
  "bannerLabel": "Classified",
  "companyName": "Your Company",
  "footerLabel": "Effectively enhancing corporate synergy",
  "footerEnabled": "false",
  "loginLogo": "(optional - base64 encoded png, 100px height)",
  "navBarLogo": "(optional - base64 encoded png, 80px height)"
}
```

Consumes

- application/json

Produces

- application/json

Path parameters

- **tid** (required)

Request body

[ApiTheme](#)

Responses

default

successful operation

url

POST /url

Create a hash for a URL

Creates and returns a hash for the specified URL.

Example Request Body

```
{
  "url": "http://localhost:3000/dashboard/0/entities?ts=-2660400&te=133024&q=&dashboard=ts%3D-2660400%26te%3D133024%26q%3D"
}
```

Example Response (Status 200)

```
{
  "hash": "89653e5d"
}
```

Produces

- application/json

Request body

[ApiUrl](#)

Return type

[ApiHash](#)

Example data

Content-Type: application/json

```
{
  "hash" : "hash"
}
```

Responses

200

successful operation

GET /url/{hash}

Redirect to the URL for a hash

Redirects the user interface to the URL associated with the specified hash.

Produces

- application/json

Path parameters

- **hash** (required)
The URL's hash.

Responses

default

successful operation

users

GET /users

Get the list of users

Gets the list of all users.

Produces

- application/json

Return type

array[Tenant]

Example data

Content-Type: application/json


```
[ {  
  "created" : "2000-01-23T04:56:07.000+00:00",  
  "tenantId" : "a3b",  
  "name" : "Interaset"  
}, {  
  "created" : "2000-01-23T04:56:07.000+00:00",  
  "tenantId" : "a3b",  
  "name" : "Interaset"  
} ]
```

Responses

200

successful operation

Models

ApiAction

- **success** -- Boolean
- **detail** -- String

ApiCredentials

- **username** -- String
- **password** -- String

ApiDashboard

- **doc** -- String
- **name** -- String
- **description** -- String
- **tid** -- String

- **userId** -- String
- **id** -- Integer
Format: int32
- **lastModifiedBy** -- String
- **creationDate** -- Date
Format: date-time
- **lastModifiedDate** -- Date
Format: date-time
- **home** -- Boolean
- **tags** -- array[ApiDashboardTag]
- **private** -- Boolean

ApiDashboardTag

- **name** -- String
A name for the tag.
- **id** -- String
Tag ID

ApiEntityNameRequest

- **entityName** -- String
- **entityType** -- String

ApiHash

- **hash** -- String

ApiMetaRequest

- **resourceType**(*Required*) -- String
The type of the meta resource e.g. comment, annotation, tag, dashboard, visualization and so on.
Enumeration:
 - comment
 - annotation
 - dashboard
 - tag
 - tuning
 - anomalySeen
- **destinationId**(*Required*) -- String
The ID of the destination.
- **destinationType**(*Required*) -- String
The type of the source. Currently supported
Enumeration:
 - alerts
 - anomalies
 - entities
- **content**(*Required*) -- String
The raw content of the object. This is a full text search. Larger than 128KB can significantly impact the search performance.
- **contentType**(*Required*) -- String
Currently supported: markdown, plaintext, html
Enumeration:
 - plaintext
 - markdown
 - json
 - html

ApiSavedSearches

- **name** -- String
- **doc** -- JsonNode
- **columns** -- JsonNode

ApiSavedSearchesDraft

- **docDraft** -- JsonNode
- **columnsDraft** -- JsonNode

ApiSavedSearchesResponse

- **name** -- String
- **doc** -- JsonNode
- **columns** -- JsonNode
- **id** -- Integer
Format: int32
- **docDraft** -- JsonNode
- **columnsDraft** -- JsonNode

ApiSessionTenant

- **userId** -- String
The user ID.
- **tenantId** -- String
The tenant ID.
- **permission** -- array[String]
The user's permissions for this tenant.
Enumeration:
- **tenantName** -- String

The tenant name.

- **features** -- array[String]

A list of UI configuration features.

ApiSimpleDashboard

- **doc** -- String
- **name** -- String
- **description** -- String
- **private** -- Boolean

ApiSimpleDashboardTag

- **name** -- String
- A name for the tag.

ApiTagEntities

- **entities** -- array[String]

ApiTenantUser

- **userId** -- String
The user ID.
- **tenantId** -- String
The tenant ID.
- **name** -- String
The user's display name.
- **role** -- String
The user's role for this tenant. The role determines the permissions for the user.

Enumeration:

- user
- admin
- root
- none

- **permissions** -- array[String]

The user's permissions for this tenant.

Enumeration:

- **isActive** -- Boolean
When `false`, this user has been marked as inactive in an external authentication service.
- **password** -- String
- **created** -- Long
The date in milliseconds when this user was created. Format: int64
- **persistentSessions** -- Boolean
When set to `true`, sessions will not expire for this user.
- **local** -- Boolean
When set to `true`, this user is local.

ApiTheme

- **loginGradient1** -- String
- **loginGradient2** -- String
- **accent** -- String
- **navBar** -- String
- **font1** -- String
- **font2** -- String
- **font3** -- String
- **banner** -- String
- **bannerLabel** -- String
- **companyName** -- String

- **footerLabel** -- String
- **footerEnabled** -- Boolean
- **loginLogo** -- String
- **navBarLogo** -- String

ApiUrl

- **url** -- String

DbUser

- **userId** -- String
- **name** -- String
- **isActive** -- Boolean
- **passwordHash** -- String
- **passwordSalt** -- String
- **timestamp** -- Date
Format: date-time
- **persistentSessions** -- Boolean
- **properties** -- map[String, String]

JsonNode

- **valueNode** -- Boolean
- **containerNode** -- Boolean
- **missingNode** -- Boolean
- **nodeType** -- String
Enumeration:

- ARRAY
- BINARY
- BOOLEAN
- MISSING
- NULL
- NUMBER
- OBJECT
- POJO
- STRING
- **pojo** -- Boolean
- **number** -- Boolean
- **integralNumber** -- Boolean
- **floatingPointNumber** -- Boolean
- **short** -- Boolean
- **int** -- Boolean
- **long** -- Boolean
- **float** -- Boolean
- **double** -- Boolean
- **bigDecimal** -- Boolean
- **bigInteger** -- Boolean
- **textual** -- Boolean
- **boolean** -- Boolean
- **binary** -- Boolean
- **object** -- Boolean
- **array** -- Boolean
- **empty** -- Boolean
- **null** -- Boolean

LoginResponse

- **access_token** -- String
Access token.
- **token_type** -- String
Token type (e.g., Basic, Bearer); usually Bearer.

RawEventsGraphRequest

- **query** -- JsonNode
- **sortFields** -- array[SortField]
- **datasources** -- array[String]
Enumeration:
- **ts** -- Long
Format: int64
- **te** -- Long
Format: int64
- **grouping** -- String
- **fields** -- array[String]

RawEventsRequest

- **query** -- JsonNode
- **sortFields** -- array[SortField]
- **datasources** -- array[String]
Enumeration:
- **ts** -- Long
Format: int64
- **te** -- Long

Format: int64

RawEventsTypeaheadRequest

- **query** -- JsonNode
- **sortFields** -- array[SortField]
- **datasources** -- array[String]

Enumeration:

- **ts** -- Long
Format: int64
- **te** -- Long
Format: int64
- **count** -- Integer
Format: int32
- **field** -- String
- **text** -- String
- **sort** -- String

Enumeration:

- asc
- desc

ServiceProxyInfo

- **schema** -- String
- **prefix** -- String
- **description** -- String
- **menu** -- String
- **permissionsByMethod** -- map[String, String]

Enumeration:

- **name** -- String

Session

- **user** -- DbUser
- **accessToken** -- String
- **expirationDate** -- Date
Format: date-time
- **maxSessionAge** -- Integer
Format: int32
- **permissionsPerTenant** -- map[String, array[String]]
Enumeration:

SessionInfo

- **userId** -- String
The user ID.
- **userDisplayName** -- String
The user's display name.
- **extendedApi** -- array[ServiceProxyInfo]
The available proxied APIs.
- **persistentSessions** -- Boolean
When set to true, sessions will not expire for this user.
- **disableTenantManagement** -- Boolean
When set to true, multi-tenant support is disabled.
- **accessToken** -- String
The current access token for this user
- **permissions** -- array[ApiSessionTenant]
- **analyticsTuningAvailable** -- Boolean
Set to true to allow the tuning of analytics.
- **swaggerEndpoints** -- map[String, String]

Available Swagger Endpoints

SortField

- **field** -- String
- **order** -- String

Enumeration:

- asc
- desc

TagBase

- **name** -- String
A name for the tag.
- **description** -- String
A description of the tag.
- **entities** -- array[String]

Tenant

- **tenantId** -- String
The tenant ID. Must be 1 to 3 alpha-numerical characters.
- **name** -- String
The tenant name.
- **created** -- Date
The tenant creation date. Format: date-time

Exports API Reference

Version: 6.4.5

BasePath: /exports

The Exports API provides a mechanism for exporting reports that contain the information presented in the Intelligence user interface.

Construct Exports API URLs

To call an endpoint in this API, use the fully-qualified domain name (FQDN) of Intelligence, and append the base path (/exports) followed by the path listed in the sections that follow. For example, to call the GET /info/build endpoint, use the following URL with the GET method:

```
https://<FQDN of Intelligence>/exports/info/build
```

Exports API Endpoints

GET /dashboard

Get risk report

Generates a detailed report of the organizational risk, including sections for Top Anomalies and Violations, Top Risky Users, Top Risky Projects, and so on.

Consumes

- application/json

Produces

- application/pdf

Query Parameters

- **tid**
The tenant ID.
- **format**
The format of the exported dashboard (pdf, jpeg, or png).

- **ts**
Start time in seconds. If no value is provided, the start time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **te**
End time in seconds. If no value is provided, the end time of the dataset is used. You can also use (case-insensitive) natural language with relative times, for example, 'first monday in july, 2017', or '10 days ago'.
- **tz**
The timezone in which the results should be returned (e.g., +5:00, America/Montreal, EST).

Return type

String

Responses

```
200 OK
```

Successful operation

GET /info/build

Get version information

Returns information about this version of the Exports API.

Example Response (Status 200)

```
{"Build-Number": "5.7.0.937"}
```

Produces

application/json

Responses

```
200 OK
```

Successful operation

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on ArcSight Intelligence SaaS 6.4.5 Developer's Guide

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!