Mandiant

SEARCH SYNTAX FOR ATTACK SURFACE MANAGEMENT

The Mandiant Advantage Attack Surface Management (MA-ASM) search syntax operates under a few simple rules:

- Queries of different keywords are AND'd

  For example: `acme.com port_tcp:80`
  Read this as "any Entity with acme.com in the name AND port 80 TCP open"

- Queries of the same keyword are OR'd

  For example: `acme.com port_tcp:80 port_tcp:443`
  Read this as "any Entity with acme.com in the name AND (port 80 TCP OR port 443 TCP open)"

- For negative queries, use `!` (NOT) before the search parameter, or search term

  For example: `type:!uri`
  Read this as "any type but NOT uri"

  The `!` (NOT) works in Issues, Entities, and Technologies but does not work with
  - Specific date filters like `last_seen_after`, `last_seen_before`, and `first_seen_after`
  - Collection filters

- The default search field (when no keyword is specified) is the item's "name" (for each of Entity, Issue, and Technology search)

Search Keywords

When searching on the **Issues**, **Entities**, and **Technologies** pages, you can create sophisticated queries using the keyword search, in addition to regular text searches. Accepted search terms together with their applicability on the **Issues**, **Entities**, and **Technologies** pages are defined below.

Search Keyword	Pretty Text (may differ from keyword)	Input	Issues	Entities	Technologies
key: `collection`		a Collection	✔	✔	
key: `confidence`	Confidence	Confirmed, Potential	✔		
key: `entity_type`	Entity Type	Text	✔	✔	
key: `entity_name`	Entity Name	Text	✔		
key: `last_seen_after`	Last seen after	YYYY-MM-DD, `last_scan_count_NUMBER` (where `NUMBER` = 1-10)	✔	✔	✔

Search Keyword	Pretty Text (may differ from keyword)	Input	Issues	Entities	Technologies
key: `last_seen_before`	Last seen before	YYYY-MM-DD, `last_scan_count_NUMBER` (where `NUMBER` = 1-10)	✔	✔	✔
key: `first_seen_after`	First seen after	YYYY-MM-DD, `last_scan_count_NUMBER` (where `NUMBER` = 1-10)	✔	✔	✔
key: `scoped`	Scoped	True, False, Both	✔	✔	
key: `severity`	Severity	`1` (critical), `2` (high), `3` (medium), `4` (low), `5` (informational)	✔		
key: `severity_lt`	Severity is less than	1 - 5	✔		
key: `severity_gt`	Severity is greater than	1 - 5	✔		
key: `status_new`	Issues	Open, Closed	✔		
key: `status`	Status is	open_triaged, open_in_progress, closed_mitigated, closed_resolved, closed_duplicate, closed_out_of_scope, closed_benign, closed_risk_accepted, closed_false_positive, closed_no_reproduce, closed_tracked_externally	✔		
key: `cisa_kev`	CISA KEV	True, False	✔		
key: `type`		Text		✔	
key: `name`	Name	Text		✔	✔
key: `tag`	Tag	Text	✔	✔	
key: `country`	Country	Two letter code, *ex:* FR		✔	
key: `hidden`	Hidden	True, False, Both		✔	
key: `http_code`	HTTP Code	Text		✔	
key: `http_auth`	HTTP Auth	True, False		✔	
key: `http_auth_basic`	Has basic auth	True, False		✔	

Search Keyword	Pretty Text (may differ from keyword)	Input	Issues	Entities	Technologies
key: `http_auth_ntlm`		True, False		✔	
key: `http_title`	HTTP Title	Text		✔	
key: `http_forms`	Form detected on URI	True, False		✔	
key: `technology`	Technology	Text		✔	
key: `network`	Network	Text		✔	
key: `port_tcp`		Text		✔	
key: `port_udp`		Text		✔	
key: `issue_count_lt`	Has issue count less than	Number		✔	
key: `issue_ count_gt`	Has issue count greater than	Number		✔	
key: `cpe`	CPE	Text		✔	✔
key: `label`	Label	Text			✔
key: `cpe_type`	CPE Type	application, service, hardware, os			✔
key: `product`	Product	Text			✔
key: `vendor`	Vendor	Text			✔
key: `version`		version number			✔
key: `cve_inferred`		a CVE		✔	
key: `cve_confirmed`		a CVE		✔	
key: `seed`	Seed	True, False		✔	
key: `critical_or_high`	Critical or High	an Entity		✔	