Mandiant

EXPORT SEARCH RESULTS

Exported search results in Mandiant Advantage Attack Surface Management (MA-ASM) contain raw data used for the platform to display related content such as the list of **Issues** (https://docs.mandiant.com/home/asm-issues), **Entities** (https://docs.mandiant.com/home/asm-entities), and **Technologies** (https://docs.mandiant.com/home/asm-technologies). Some fields are intentionally left blank. The content fields can be exported into a PDF, CSV, or JSON file. Exported files contain all fields associated with your search results.

Export search results

1. In MA-ASM, select the **Issues, Entities**, or **Technologies** tab.
2. Select the relevant search **Filters**, making adjustments as needed to refine the scope.

   - Existing search results are exported. Therefore, before exporting, you must run searches using your required search criteria.
   - For best results, limit CSV and JSON exports to 150,000 Issues, Entities, or Technologies.
   - PDF exports are limited to 3,000 Issues or Entities.

3. Click **Export**.
   - For Issues and Entities select an option:
     - **Export As CSV + JSON**
     - **Generate PDF**
   - For Technologies select **Export As CSV + JSON**

   Once you select an Export option, you are notified that the export is in progress. When the export is complete, you receive an email containing a link to the file.

View Download Exports

A comprehensive table of previously requested export files is available on the **Download Exports** page. From this page, each export file can be downloaded. To access **Download Exports**, take the following steps:

1. In MA-ASM, select **Exports** from your **Projects and Settings** menu.
2. Click ⋮ associated with an export file.
3. Select **Download PDF**, **Download CSV**, or **Download JSON**.

Once downloaded, files are located in the default download folder of your local machine.

Exported search results

The following tables list the exported fields for **Issues**, **Entities**, and **Technologies**.

Exported fields for Issues

Field	Description/Example
Refresh date	Example: `2023-06-03 12:15:27 UTC`
Type	
Name	

Field	Description/Example
Collection (https://docs.mandiant.com/home/asm-customize-collections) Name	
Last seen	Example: `2023-06-03T12:15:27.000Z`
First seen	Example: `2023-06-03T12:15:27.000Z`
Id	
Uid	
Uuid	
Description	Example: `When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection ...`
Dynamic Id	Example: `19247113`
Pretty Name	Example: `Apache HTTP Server Path Traversal Bypass (CVE-2021-42013)`
Upstream	The system that is associated with the issues for data collection
Entity Uid	
Entity Name	IP address and port for a server Example: `https://1.123.45.67:9443` or `12.345.678.99:22/tcp`
Alias Group	
Collection Uuid	
Collection Type	Example: `user_collection`
Organization Uuid	
Summary.Pretty Name	Example: `Apache HTTP Server Path Traversal Bypass (CVE-2021-42013)`
Summary.Severity	Severity of the Issue
Summary.Scoped	Example: `true`
Summary.Confidence	Example: `confirmed`
Summary.Status	Example: `open_new`
Summary.Category	Example: `Vulnerability`
Summary.Identifiers	Example: `[{"name"=>"CVE-2021-42013", "type"=>"CVE"}]`
Summary.Status New	Example: `open`
Summary.Status New Detailed	Example: `new`

Field	Description/Example
Summary.Tickets List	List of tickets represented as an array
Tags	Array of identifier tags
Cisa (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) Known Exploited	Example: `true`
Epss (https://www.first.org/epss/) V2 Score Lte	
Epss V2 Percentile Gte	Percentile position among the total numbers
Proof	Example: `{"additional_info":"The Tomcat instance was identified vulnerable as a successful connection was made to the AJP Connector."}`
Remediation	Example: `Disable`
References	Example: `[{"uri"=>"https://www.chaitin.cn/en/ghostcat", "type"=>"description"}, {"uri"=>"https://www.tenable.com/blog/cve-2020-1938-ghostcat-apache-tomcat-ajp-file-readinclusion-vulnerability-cnvd-2020-10487", "type"=>"description"}, {"uri"=>"https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi", "type"=>"exploit"}, ...]`
Notes	An array of notes.
Collection Pretty Name	Example: `Abc AWS Network`

Exported fields for Entities

Field	Description/Example
Refresh date	Example: `2023-06-03 12:15:27 UTC`
Type	
Name	
Collection Name	
Last seen	Example: `2023-06-03T12:15:27.000Z`
First seen	Example: `2023-06-03T12:15:27.000Z`
# Issues	Example: `0`
Id	
Uid	
Uuid	
Dynamic Id	
Tags	Array of identifier tags

Field	Description/Example
Issues	Array of Issues associated with the Entity
Hidden	Example: `false`
Seed (https://docs.mandiant.com/home/asm-seeds)	Whether the Entity is considered as a Seed. Example: `false`
Aliases	
Alias Group	
Collection Type	Example: `user_collection`
Collection Naics	As per the North American Industry Classification System.
Collection Uuid	
Organization Uuid	
Exfil (https://attack.mitre.org/tactics/TA0010/#:~:text=Exfiltration%20consists%20of%20techniques%20that,can%20include%20compression%20and%20encryption.) Lookup Identifier	The identifier used for looking up data exfiltration associated with the Entity
Summary.Scoped	Example: `false`
Summary.Issues.Current With Cve	
Summary.Issues.Current By Severity.0	
Summary.Issues.Current By Severity.1	
Summary.Issues.Current By Severity.2	
Summary.Issues.Current By Severity.3	
Summary.Issues.Current By Severity.4	
Summary.Issues.Current By Severity.5	
Summary.Issues.All Time By Severity.0	

Field	Description/Example
Summary.Issues.All Time By Severity.1	
Summary.Issues.All Time By Severity.2	
Summary.Issues.All Time By Severity.3	
Summary.Issues.All Time By Severity.4	
Summary.Issues.All Time By Severity.5	
Summary.Issues.Current Count	
Summary.Issues.All Time Count	
Summary.Issues.Critical Or High	
Summary.Task Results	
Summary.Screenshot Exists	
Summary.Http.Code	
Summary.Http.Title	
Summary.Http.Content.Favicon Hash	
Summary.Http.Content.Hash	
Summary.Http.Content.Forms	
Summary.Http.Auth.Any	
Summary.Http.Auth.Basic	
Summary.Http.Auth.Ntlm	
Summary.Http.Auth.Forms	
Summary.Http.Auth.2fa	
Summary.Ports.Tcp	
Summary.Ports.Udp	
Summary.Ports.Count	

Field	Description/Example
Summary.Technology.Cloud	
Summary.Technology.Cloud Providers	
Summary.Technology.Cpes	
Summary.Technology.Technologies	
Summary.Technology.Technology Labels	
Summary.Network.Name	
Summary.Network.Asn	
Summary.Network.Route	
Summary.Network.Type	
Seeds	Example: `[{"name"=>"acme", "type"=>"Intrigue::Entity::UniqueKeyword"}]`
Notes	An array of notes.
Ports	

Exported fields for Technologies

Field	Description/Example
Refresh date	Example: `2023-06-03 12:15:27 UTC`
Name	Example: `Microsoft Sharepoint 16.0.0.23717`
Collection Name	
Last seen	Example: `2023-06-03T12:15:27.000Z`
First seen	Example: `2023-06-03T12:15:27.000Z`
Id	
Uid	
Uuid	
Dynamic Id	
Version	Released version number Example: `16.0.0.23717`

Field	Description/Example
Cpe (https://nvd.nist.gov/products/cpe) Type	Example: `application`
Cpe (https://nvd.nist.gov/products/cpe)	CPE identifiers are commonly used to search for Common Vulnerabilities and Exposures (CVEs) that affect the identified product Example: `cpe:2.3:a:microsoft:sharepoint:16.0.0.23717:`
Collection Uuid	
Collection Type	Example: `user_collection`
Update	
Vendor	Vendor for the Technology Example: `Microsoft`
Product	Product name Example: `Sharepoint`
Organization Uuid	
Updated At	Example: `2023-06-03T12:15:27.000Z`
Labels	Example: `["cots", "e-commerce", "javascript", "payments"]`