Mandiant

JOB EXPORT FIELDS

Single Job Export Report Fields

Field Title	Description	Field Format	Endpoint	Network	Email	DNS	Protected Theater	Captive IOC
Job ID	ID of the Job that was run	Integer	✔	✔	✔	✔	✔	✔
Job Step	Order of the Job that was run	Integer	✔	✔	✔	✔	✔	✔
VID	Validation Identifier of the Job	String	✔	✔	✔	✔	✔	✔
Action Name	Name of the Action	String	✔	✔	✔	✔	✔	✔
Action Description	Description of the Action	Text	✔	✔	✔	✔	✔	✔
Attack Location	Location where the Action will attack from	String	✔	✔	✔	✔	✔	✔
Attack Vector	Method the Security Validation Platform used to process the Action	String	✔	✔	✔	✔	✔	✔
Behavior Type	Type of behavior the Action will process	String	✔	✔	✔	✔	✔	✔
Stage of Attack	Attack lifecycle stage the Action belongs to	String	✔	✔	✔	✔	✔	✔
Tags	Tag(s) that categorize the Action	String	✔	✔	✔	✔	✔	✔
User Profile	User profile of user created for use with the Action	Text	✔	✔	✔	✔	✔	✔
Blocked?	Indicates whether Action was blocked (shows Yes or No)	Boolean	✔	✔	✔	✔	✔	✔

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Field Title	Description	Field Format	Endpoint	Network	Email	DNS	Protected Theater	Captive IOC
Events?	Indicates whether there were events detected	Boolean	✔	✔	✔	✔	✔	✔
Host Events	Indicates whether there were events detected from the integration	Text	✔				✔	
Source Actor	Indicates source Actor (IP address of source Actor)	String	✔	✔	✔	✔	✔	✔
Destination Actor	Indicates destination Actor (IP address of destination Actor	String	✔	✔	✔	✔	✔	✔
Target Status	Status of target	Hash/Object with key/value pairs	✔	✔	✔	✔	✔	✔
Attacker Status	Status of attacker	String	✔	✔	✔	✔	✔	✔
Proxied?	Indicates whether the Actoris a proxy (shows Yes or No)	Boolean	✔	✔	✔	✔	✔	✔
Start Run Time	When Job report was started	Boolean	✔	✔	✔	✔	✔	✔
Stop Run Time	When Job report stopped	String	✔	✔	✔	✔	✔	✔
Action Port Numbers	Attack ports	String	✔	✔	✔	✔	✔	✔
Run Time Parameters	Parameters specific to the Action	String	✔	✔	✔	✔	✔	✔
Devices	Device(s) the Action was run on	Text	✔				✔	

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Field Title	Description	Field Format	Endpoint	Network	Email	DNS	Protected Theater	Captive IOC
Correlation Rules	Rules or conditions that act as a trigger to take specific actions if a particular event occurs	String						
Filename	Filename of the Action	Text		✔				
SHA256	Password verification for the Action	Integer		✔				
Host CLI Log	Host CLI log file	Text	✔				✔	
Cloud Action Log	Cloud Action log file	Text						

Simple Jobs Export Report Fields

Field Title	Description	Field Format
Job ID	IDs of the Jobs that were run	Integer
Job Name	Names of the Jobs that were run	String
Time	Time that Jobs were run	String
Timestamp	Timestamp for when Jobs were run	String
Progress	Progress of Jobs reports, per Job (for example, **Completed Group**)	String
Status	Status of Jobs reports, per Job (for example, **Completed**)	String
User	User who ran Jobs Report	String
Description	Description of Job	Text

Job Action Report Fields

Field Title	Description	Field Format
Job ID	ID of Jobs that were run	Integer that could be a string
Job Step	Order of the Jobs that were run	Integer
Job Name	Names of Jobs that were run	String
Timestamp	Timestamp for when Jobs were run	String

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Field Title	Description	Field Format
Progress	Progress of Jobs reports, per Job (for example, value could be **Completed Group**)	String
Blocked	Whether Actions were blocked (value is **TRUE**, **FALSE**, or other message)	Boolean
Detected	Whether Actions were detected (value is **TRUE** or **FALSE**, or other message)	Boolean
Status	Status of Jobs reports, per Job (for example, **Completed**)	String
User	User who ran Jobs report	String
Action Name	Name of Action, per Job	String
VID	VID of Action, per Job	String
Action Description	Description of Action, per Job	Text
Description	Description of what the Action will do and other information, per Job	Text
Action Type	Type of Action	String
Filename	Filename of the Action, per Job	String
SHA256	Password verification for the Action	String
Action Tags	Any tags used by the Action	String
User Tags	Any tags used by the user	String
Target Status	Target status for Action	String
Attacker Status	Status of Attacker, per Job	String
Host CLI Log	Host CLI log file, per Job	Text
<Integration> Events	Events listed per Integration (for example, **Azure Sentinel**, **Elasticsearch**)	Text of events, each separated by a new line
Host CLI Events	Indicates whether there were events detected from the integration, per Job	Text of events, each separated by a new line

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.