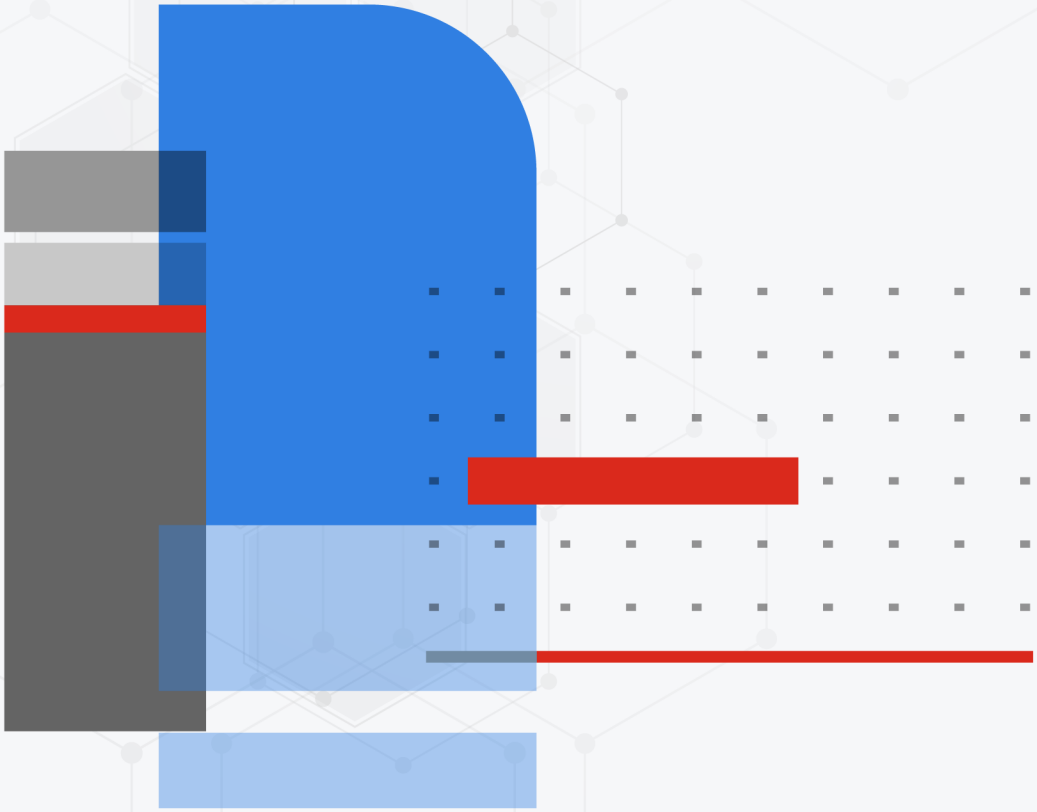
Playbook Variables

FortiAnalyzer 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 16, 2023
FortiAnalyzer 7.4.0 Playbook Variables
00-740-915098-20230516

TABLE OF CONTENTS

Change Log

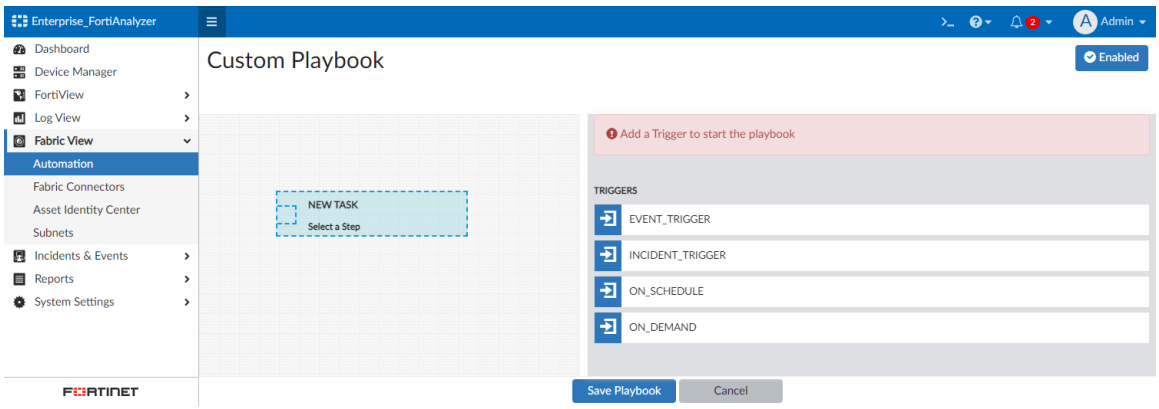
Date	Change Description
2023-05-16	Initial release.

Introduction

This document describes the trigger and output variables that can be used when configuring playbook tasks in FortiAnalyzer.

Trigger variables

Trigger variables allow you to use information from the trigger (starter) of a playbook when it has been configured with an incident trigger or event trigger.



Event trigger variables

Variable	Format	Description
devid	${trigger.devid}	Device ID
devtype	${trigger.devtype}	Device type
dst_epid	${trigger.dst_epid}	Destination endpoint ID
dst_epip	${trigger.dst_epip}	Destination endpoint IP
dst_epmac	${trigger.dst_epmac}	Destination endpoint MAC
dst_epname	${trigger.dst_epname}	Destination endpoint name
dst_fctuid	${trigger.dst_fctuid}	Destination FortiClient UID
dvid	${trigger.dvid}	The dvid is an integer that represents devid+VDOM
epid	${trigger.epid}	Endpoint ID
epip	${trigger.epip}	Endpoint IP
epmac	${trigger.epmac}	Endpoint MAC
epname	${trigger.epname}	Endpoint name
euid	${trigger.euid}	End user ID
euname	${trigger.euname}	End user name

Variable	Format	Description
event_id	${trigger.event_id}	Event ID
event_status	${trigger.event_status}	Event status
event_time	${trigger.event_time}	Event time
event_type	${trigger.event_type}	Event type
extrainfo	${trigger.extrainfo}	Extra information
fctuid	${trigger.fctuid}	FortiClient UID
groupby1	${trigger.groupby1}	Groupby1
groupby2	${trigger.groupby2}	Groupby2
groupby3	${trigger.groupby3}	Groupby3
handler_name	${trigger.handler_name}	Handler name
handler_type	${trigger.handler_type}	Handler type
indicator	${trigger.indicator}	Indicator
logtype	${trigger.logtype}	Log type
rule_name	${trigger.rule_name}	Rule name
severity	${trigger.severity}	Severity
subject	${trigger.subject}	Subject
subtype	${trigger.subtype}	Subtype
tag	${trigger.tag}	Tag
threat_type	${trigger.threat_type}	Threat type
vdom	${trigger.vdom}	VDOM

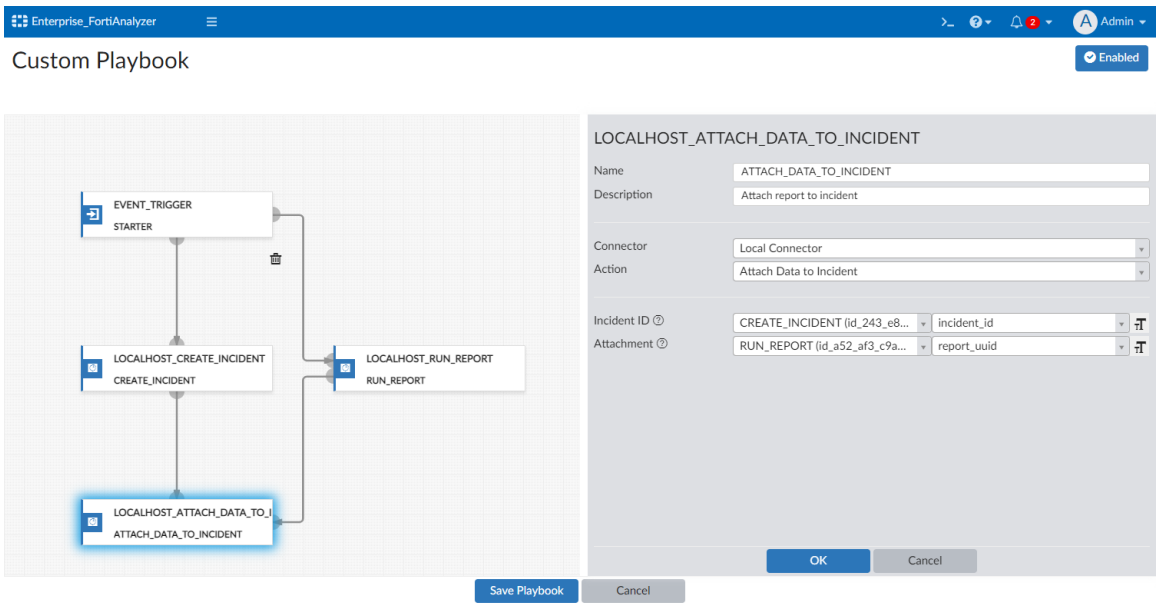
Incident trigger variables

Variable	Format	Description
assigned_to	${trigger.assigned_to}	Assigned to (new/update assigned to)
attach_revision	${trigger.attach_revision}	Attach revision (new/update/delete revision)
category	${trigger.category}	Category (new/update category)
change_type	${trigger.change_type}	Change type (new/update/delete change type)
description	${trigger.description}	Description (new/update description)

Variable	Format	Description
endpoint	${trigger.endpoint}	Endpoint (new/update endpoint)
epid	${trigger.epid}	Endpoint ID (new/update endpoint ID)
euid	${trigger.euid}	End user ID (new/update end user ID)
incident_id	${trigger.incident_id}	Incident ID (new/update/delete incident)
reporter	${trigger.reporter}	Reporter (new reporter)
revision	${trigger.revision}	Revision (new/update/delete revision)
severity	${trigger.severity}	Severity (new/update severity)
status	${trigger.status}	Status (new/update status)

Output variables

Output variables allow you to use the output from a preceding task as an input to the current task. For example, the report generated in one task can be attached to an incident in a second task.



The following format is used:

Connector Type	Action	Variable	Description
FortiAnalyzer	Create Incident	revision	Create revision
FortiAnalyzer	Get EPEU from Incident	epeu	EPEU is a JSON data structure with all related endpoint and enduser info in it: epid, epname, epip, epmac, fluid, etc.
FortiAnalyzer	Run Report	report_uuid	Run report
FortiAnalyzer	Attach Data to Incident	attach_ids	Attach data to incident
FortiAnalyzer	Update Incident	attach_revision	Attach revision
FortiAnalyzer	Update Incident	revision	Revision
FortiAnalyzer	Update Incident	incident_id	Update incident
FortiAnalyzer	Create Incident	attach_revision	Attach revision
FortiAnalyzer	Create Incident	incident_id	Create incident
FortiAnalyzer	Get Events	events	Get events matching filter conditions
FortiCASB	Get Cloud Data	No output variable	Obtain app info from FortiCASB

Connector Type	Action	Variable	Description
FortiClient EMS	Get Endpoints	ems_endpoints	List of endpoints returned from EMS server
FortiClient EMS	Tag Endpoints	No output variable	Tag endpoints
FortiClient EMS	Get Vulnerabilities	vulnerabilities	Retrieve list of vulnerabilities on an endpoint
FortiClient EMS	Get Process List	processes	Retrieve list of running processes on an endpoint
FortiClient EMS	Get Software Inventory	software	Retrieve software list installed on an endpoint
FortiClient EMS	AV Full Scan	status	Request AV full scan on an endpoint
FortiClient EMS	AV Quick Scan	status	Request AV quick scan on an endpoint
FortiClient EMS	Vulnerability Scan	status	Request vulnerability scan on an endpoint
FortiClient EMS	Unquarantine	status	Request to unquarantine an endpoint
FortiClient EMS	Quarantine	status	Request to quarantine an endpoint
FortiClient EMS	Untag Endpoints	No output variable	Untag endpoints
FortiGuard	Lookup Indicator	indicators	Threat intelligence indicators
FortiMail	Get Email Statistics	statistics	Get email statistics for a given email address
FortiMail	Get Sender Reputation	reputation	Get sender reputation statistics for a given email address
FortiMail	Add Sender to Blocklist	No output variable	Add sender to blocklist (system and domain level)
FortiOS	Webhook	No output variable	Webhook call towards FortiOS
MS_TEAMS	Send Message	No output variable	Send message in Microsoft Teams
ServiceNow	Post Incident Change Notice	No output variable	Post incident change notice to ServiceNow

We can get a different variable output even if the action is the same by referring to different macros. For example:

```
${create_incident_task_id.revision}
${create_incident_task_id.attach_revision}
```

www.fortinet.com