SOC Automation Objects

FortiAnalyzer 8.0.0

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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 29, 2026
FortiAnalyzer 8.0.0 SOC Automation Objects
05-800-1077324-20260529

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-11-12	Initial publication.
2025-12-05	Release of content pack v25.11002.
2025-12-22	Release of content pack v25.12003.
2026-01-30	Release of content pack v26.01002.
2026-03-04	Release of content pack v26.02002.
2026-04-01	Release of content pack v26.03005.
2026-04-06	Updated Introduction on page 8.
2026-04-21	Release of FortiAnalyzer 8.0.
2026-05-01	Release of content pack v26.04003.
2026-05-29	Release of content pack v26.05003.

Introduction

The FortiAnalyzer Security Automation Service is a license that provides content packs released from FortiGuard on a monthly basis. The content packs include premium reports, advanced correlation rules, third-party log parsers, and more. These tools are designed to help you detect, investigate, and respond to security incidents. With a valid Security Automation Service license, the content pack release is applied automatically in FortiAnalyzer when it is available from the FortiGuard distribution server.

Beginning in FortiAnalyzer 7.4.9 and 7.6.5, FortiAnalyzer requires a valid FortiCare Elite or FortiCare Premium support contract registered in FortiCloud in order to get object updates from FortiGuard. This includes the SOC Automation objects described in this guide.

For more information, see SOC Automation in the FortiAnalyzer Administration Guide.

Log parsers

This section provides details about the log parsers added as part of the FortiAnalyzer Security Automation Service. The log parsers can be used to normalize logs from thrid-party devices/services and insert them into the SIEM database (siemdb). Once inserted, these logs can be viewed in Log View, and they can be used in custom event handlers and reports.

The topics in this section list the fields from the third-party logs and the normalized field that it maps to once parsed and inserted into the siemdb.

Armis Platform logs

FortiAnalyzer supports normalizing Armis Platform logs as Fabric logs.

This log parser normalizes Armis CEF logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Armis Platform Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
app	app_name
destIpAddr	dst_ip
destMACAddr	dst_mac
activityName	event_action
msg_body	event_message
devEventTypeGrp	event_profile
title	event_ref
eventSeverity	event_severity
log_subtype	event_subtype
eventType	event_type
log_type	event_cat

Armis Platform Log Field	Normalized Fabric Log Field
reptDevName	host_name
infoURL	http_url
ipProto	net_proto
srcIpAddr	src_ip
srcMACAddr	src_mac
srcIpPort	src_port
userId	user_id
srcUser	user_name

Aruba ClearPass Policy Manager (CPPM) logs

FortiAnalyzer supports normalizing Aruba ClearPass Policy Manager (CPPM) logs as Fabric logs.

Aruba ClearPass Policy Manager (CPPM) is a Network Access Control (NAC) platform that provides role-based policies for authentication, authorization, accounting (AAA), endpoint profiling, policy decisions, security posture assessments, and system-level events.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Aruba ClearPass Policy Manager (CPPM) Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,device_timestamp,dtime	data_timestamp
serviceName	app_service
destIpAddr	dst_ip
eventAction	event_action
msg_body,message	event_message
eventSeverity	event_severity
eventType	event_type
host_ip	host_ip

Aruba ClearPass Policy Manager (CPPM) Log Field	Normalized Fabric Log Field
hostMACAddr	host_mac
netProto	net_proto
srcIpAddr	src_ip
nepDevIpAddr	src_natip
user	user_name

Aruba CX logs

FortiAnalyzer supports normalizing Aruba CX logs as Fabric logs.

This log parser normalizes Aruba-CX logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Aruba CX Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
hostVLAN	dst_domain
intfName	dst_intf
eventAction	event_action
event_id	event_id
msg_body	event_message
errorString	event_outcome
event_ref	event_ref
eventSeverity	event_severity
eventType	event_type
event_cat	event_cat
reptDevName	host_name
src_ip	src_ip

Aruba CX Log Field	Normalized Fabric Log Field
srcMACAddr	src_mac
user	user_id
user	user_name

AWS CloudTrail logs

FortiAnalyzer supports normalizing AWS CloudTrail logs as Fabric logs.

AWS CloudTrail records all API calls and management actions made in an AWS account, across AWS services, and delivers them as JSON event logs.

Requirement:

- FortiAnalyzer 7.6.3 or later

The following field mapping applies:

AWS CloudTrail Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
data_sourcetype	data_sourcetype
data_sourceversion	data_sourceversion
data_timestamp,itime	data_timestamp
dst_domain	dst_domain
event_action	event_action
event_cat	event_cat
event_error	event_error
event_message	event_message
event_name	event_name
event_outcome	event_outcome
event_policy	event_policy
event_profile	event_profile
msg	event_rawmsg
event_ref	event_ref
event_resource_group	event_resource_group
event_source	event_source

AWS CloudTrail Log Field	Normalized Fabric Log Field
event_status	event_status
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
host_location	host_location
host_type	host_type
host_uid	host_uid
http_useragent	http_useragent
src_ip	src_ip
tls_cipher	tls_cipher
tls_version	tls_version
user_domain	user_domain
user_group	user_group
user_id,account_id	user_id
user_id_name,user_name,target_user	user_name
user_id_role,user_role	user_role

AWS CloudWatch logs

FortiAnalyzer supports normalizing AWS CloudWatch logs as Fabric logs.

AWS CloudWatch collects and monitors system, application, and custom log files, and delivers them as structured JSON logs.

Requirement:

- FortiAnalyzer 7.6.3 or later

The following field mapping applies:

AWS CloudWatch Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
data_sourcetype	data_sourcetype
data_sourceversion	data_sourceversion

AWS CloudWatch Log Field	Normalized Fabric Log Field
cw_ts,itime	data_timestamp
dst_domain	dst_domain
event_action	event_action
event_cat	event_cat
event_creation_time	event_creation_time
event_error	event_error
event_error_code	event_error_code
event_message	event_message
event_name	event_name
event_outcome	event_outcome
event_policy	event_policy
event_profile	event_profile
raw_msg,msg	event_rawmsg
event_ref	event_ref
event_resource_group	event_resource_group
event_source	event_source
event_status	event_status
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
host_location	host_location
host_type	host_type
host_uid	host_uid
http_useragent	http_useragent
src_domain	src_domain
src_ip	src_ip
tls_cipher	tls_cipher
tls_version	tls_version

AWS CloudWatch Log Field	Normalized Fabric Log Field
user_domain	user_domain
user_group	user_group
user_id,account_id,target_account_id	user_id
user_id_name,user_name,caller_name,target_user	user_name
user_id_role,user_role	user_role

AWS Security Hub logs

FortiAnalyzer supports normalizing AWS Security Hub logs as Fabric logs.

AWS Security Hub Cloud Security Posture Management (CSPM) consumes and aggregates findings from integrated AWS services and third-party products. This log parser normalizes logs ingested from the AWS Security Hub Connector.

Requirement:

- FortiAnalyzer 7.6.3 or later

The following field mapping applies:

AWS Security Hub Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename	data_sourcename
msg_tag	data_sourcetags
data_sourcetype	data_sourcetype
aws_account_id	data_sourceuuid
created_time	data_timestamp
data_version	data_version
aws_account_id	cloud_username
event_action	event_action
event_cat	event_cat
event_count	event_count
created_time	event_creation_time
event_first_seen_time	event_first_seen_time
event_last_seen_time,updated_time	event_last_seen_time

AWS Security Hub Log Field	Normalized Fabric Log Field
event_message	event_message
event_name	event_name
event_profile	event_profile
msg	event_rawmsg
event_ref	event_ref
event_report_url	event_report_url
event_resource_group	event_resource_group
event_resource_id	event_resource_id
event_severity	event_severity
event_source	event_source
event_status	event_status
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
src_geo_city	src_geo_city
src_geo_country	src_geo_country
src_geo_country_code	src_geo_country_code
src_geo_latitude	src_geo_latitude
src_geo_longitude	src_geo_longitude
src_geo_region	src_geo_region

Azure Event Hub logs

FortiAnalyzer supports normalizing Azure Event Hub logs as Fabric logs.

Azure Event Hubs provides real-time data ingestion logs for streaming pipelines, including event publishing, consumer group subscriptions, partition assignments, throughput unit utilization, and error or throttling events.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Azure Event Hub Log Field	Normalized Fabric Log Field
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
devid	data_sourceuuid
data_timestamp,dtime	data_timestamp
app_id	app_id
app_name	app_name
event_action	event_action
event_assignee	event_assignee
event_message	event_message
event_outcome	event_outcome
event_policy	event_policy
event_profile	event_profile
msg	event_rawmsg
event_resource_group	event_resource_group
event_resource_id	event_resource_id
event_severity	event_severity
event_start_time	event_start_time
event_status	event_status
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
host_ip	host_ip
host_name	host_name
host_osfamily	host_osfamily
http_method	http_method
http_response_bytes	http_response_bytes
http_status_code	http_status_code
http_url	http_url
http_useragent	http_useragent

Azure Event Hub Log Field	Normalized Fabric Log Field
src_geo	src_geo
src_geo_city	src_geo_city
src_geo_country	src_geo_country
src_geo_region	src_geo_region
src_ip	src_ip
user_email	user_email
user_group	user_group
user_id	user_id
user_name	user_name

Azure Sentinel logs

FortiAnalyzer supports normalizing Azure Sentinel logs as Fabric logs.

Azure Sentinel alerts are generated from various security solutions and can be configured to create incidents automatically, helping security teams respond effectively to potential threats. This log parser normalizes data ingested by the Azure Sentinel Connector.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Azure Sentinel Log Field	Normalized Fabric Log Field
msg_tag	data_sourcetags
data_sourcetype	data_sourcetype
data_sourceuuid	data_sourceuuid
data_timestamp,dtime	data_timestamp
event_assignee	event_assignee
event_cat	event_cat
event_creation_time	event_creation_time
event_last_seen_time	event_last_seen_time
event_message	event_message
event_name	event_name

Azure Sentinel Log Field	Normalized Fabric Log Field
msg	event_rawmsg
event_severity	event_severity
event_source	event_source
event_status	event_status
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
host_ip	host_ip
host_name	host_name
host_osname	host_osname

Barracuda Firewall logs

FortiAnalyzer supports normalizing Barracuda Firewall logs as Fabric logs.

This log parser normalizes Barracuda cloud and web application logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.6.2 or later

The following field mapping applies:

Barracuda Firewall Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
opName	cloud_appaction
appName	cloud_appname
targetDomain	dst_domain
destIntfName	dst_intf
destServiceName	dst_intf_role
destIpAddr	dst_ip
postNATDestIpAddr	dst_natip

Barracuda Firewall Log Field	Normalized Fabric Log Field
destIpPort	dst_port
fwAction	event_action
cloud_log_type	event_cat
eventID	event_id
msg	event_message
remedyAction	event_outcome
fwRule	event_policy
profileDetails	event_profile
cloud_msg_body,web_app_msg_body	event_rawmsg
webCategory	event_ref
log_severity,eventSeverityCat	event_severity
type	event_subtype
eventType	event_type
host_name	host_name
osObjName	host_osname
httpCookie	http_cookie
hostIPofServer	http_host
httpMethod	http_method
httpReferrer	http_referer
httpStatusCode	http_status_code
downloadURL	http_url
httpUserAgent	http_useragent
httpVersion	http_version
ipProto	net_proto
recvPkts	net_rcvdpkts
recvBytes	net_recvbytes
sentBytes	net_sentbytes
sentPkts	net_sentpkts
duration	net_sessionduration
srcIntfName	src_intf

Barracuda Firewall Log Field	Normalized Fabric Log Field
srcIpAddr	src_ip
srcMACAddr	src_mac
postNATSrcIpAddr	src_natip
srcIpPort	src_port
user	user_name

Brocade logs

FortiAnalyzer supports normalizing Brocade logs as Fabric logs.

This log parser normalizes Brocade logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Brocade Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
action	event_action
eventType	event_type
host_name	host_name
net_proto	net_proto
src_ip	src_ip
src_mac	src_mac
user	user_id
user	user_name

CheckPoint logs

FortiAnalyzer supports normalizing CheckPoint logs as Fabric logs.

CheckPoint firewall logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

CheckPoint Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
product	app_name
version	app_ver
dnsQuery	dns_query
dnsType	dns_querytype
destIpAddr,destIpAddr2	dst_ip
destIpPort	dst_port
eventAction,operation	event_action
chk_msg_body,cef_msg_body,gaia_msg_body,kv_msg_body	event_message
policyName	event_policy
event_profile	event_profile
errReason	event_ref
eventSeverity	event_severity
compEventType,cef_type	event_subtype
eventType	event_type
cef_product	event_cat
fileType	file_ext
fileName,scannedFiles	file_name
hostIpAddr	host_ip
hostName	host_name
osName	host_osname
osVersion	host_osver
deviceIdentification	host_uid
infoURL	http_url

CheckPoint Log Field	Normalized Fabric Log Field
subject	mail_subject
direction,fileDirection	net_direction
ipProto	net_proto
recvPkts64	net_rcvdpkts
recvBytes64	net_recvbytes
sentBytes64	net_sentbytes
sentPkts64	net_sentpkts
durationMSec	net_sessionduration
srcIntfName	src_intf
srcIpAddr	src_ip
srcIpPort	src_port
attackName	threat_name
attackInfo	threat_pattern
threat_severity	threat_severity
userDN	user_domain
userGrp	user_group
user,srcUser	user_name

Cisco Adaptive Security Appliance (ASA) logs

FortiAnalyzer supports normalizing Cisco Adaptive Security Appliance (ASA) logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Cisco ASA syslogs and normalize firewall access-control, connection/session, NAT, VPN, authentication, admin, web, threat/IPS, and system events into SIEM fields, driven by message-id specific regex extraction.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Cisco Adaptive Security Appliance (ASA) Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename

Cisco Adaptive Security Appliance (ASA) Log Field	Normalized Fabric Log Field
data_sourcetype	data_sourcetype
data_timestamp,dtime	data_timestamp
destDomain	dst_domain
destIntfName	dst_intf
destIpAddr	dst_ip
postNATDestIpAddr	dst_natip
postNATDestIpPort	dst_natport
destIpPort	dst_port
eventAction	event_action
message_id	event_id
msg_body	event_message
event_outcome	event_outcome
policyName	event_policy
event_profile	event_profile
event_severity	event_severity
eventSubType	event_subtype
eventType	event_type
fileName	file_name
reptDevIpAddr	host_ip
hostName	host_name
URL	http_url
direction	net_direction
netProto	net_proto
recvBytes64	net_recvbytes
sentBytes64	net_sentbytes
srcIntfName	src_intf
srcIpAddr	src_ip
postNATSrcIpAddr	src_natip
postNATSrcIpPort	src_natport
srcIpPort	src_port

Cisco Adaptive Security Appliance (ASA) Log Field	Normalized Fabric Log Field
userGrp	user_group
userIP	user_location
user	user_name

Cisco Duo MFA logs

FortiAnalyzer supports normalizing Cisco Duo MFA logs as Fabric logs.

Cisco Duo generates multi-factor authentication (MFA) logs including access requests, verifications, and policy enforcement.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Cisco Duo MFA Log Field	Normalized Fabric Log Field
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
devid	data_sourceuuid
data_timestamp,dtime	data_timestamp
app_id	app_id
app_name	app_name
event_action	event_action
event_assignee	event_assignee
event_message	event_message
event_outcome	event_outcome
event_policy	event_policy
event_profile	event_profile
msg	event_rawmsg
event_severity	event_severity
event_start_time	event_start_time
event_status	event_status

Cisco Duo MFA Log Field	Normalized Fabric Log Field
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
host_ip	host_ip
host_name	host_name
host_osfamily	host_osfamily
http_useragent	http_useragent
src_geo_city	src_geo_city
src_geo_country	src_geo_country
src_geo_region	src_geo_region
src_ip	src_ip
user_email	user_email
user_group	user_group
user_id	user_id
user_name	user_name

Cisco Firepower logs

FortiAnalyzer supports normalizing Cisco Firepower logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Cisco Firepower CEF syslogs and normalize firewall, connection, IPS, and threat-related fields into SIEM data. It also supports severity mapping, policy extraction, file and malware attributes, and full key-value body parsing.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Cisco Firepower Log Field	Normalized Fabric Log Field
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
devid	data_sourceuuid

Cisco Firepower Log Field	Normalized Fabric Log Field
data_timestamp,dtime	data_timestamp
app_name	app_name
dst_ip	dst_ip
dst_port	dst_port
event_action	event_action
event_cat	event_cat
event_end_time	event_end_time
event_message	event_message
event_policy	event_policy
event_policyid	event_policyid
event_profile	event_profile
msg_body	event_rawmsg
event_severity	event_severity
event_source	event_source
event_start_time	event_start_time
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
file_ext	file_ext
file_hash	file_hash
file_name	file_name
file_size	file_size
host_name	host_name
http_url	http_url
net_proto	net_proto
net_sentbytes	net_sentbytes
src_geo_city	src_geo_city
src_geo_country	src_geo_country
src_geo_region	src_geo_region
src_ip	src_ip

Cisco Firepower Log Field	Normalized Fabric Log Field
src_port	src_port
threat_name	threat_name
user_id	user_id

Cisco Identity Services Engine logs

FortiAnalyzer supports normalizing Cisco Identity Services Engine logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Cisco Identity Services Engine (ISE) authentication-authorization-accounting syslogs, and normalize user, device, and policy fields into SIEM data. It also provides full AAA visibility through comprehensive field extraction.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Cisco Identity Services Engine Log Field	Normalized Fabric Log Field
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
devid	data_sourceuuid
data_timestamp,dtime	data_timestamp
dst_ip	dst_ip
dst_mac	dst_mac
dst_port	dst_port
event_action	event_action
event_error	event_error
event_message	event_message
event_outcome	event_outcome
event_policy	event_policy
event_profile	event_profile
msg_body	event_rawmsg
event_severity	event_severity
event_status	event_status

Cisco Identity Services Engine Log Field	Normalized Fabric Log Field
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
host_ip	host_ip
host_mac	host_mac
host_name	host_name
process_command_line	process_command_line
src_geo_city	src_geo_city
src_geo_country	src_geo_country
src_geo_region	src_geo_region
src_ip	src_ip
src_mac	src_mac
src_port	src_port
user_authtype	user_authtype
user_id	user_id
user_name	user_name
user_xauthgroup	user_xauthgroup
user_xauthuser	user_xauthuser

Cisco IOS logs

FortiAnalyzer supports normalizing Cisco IOS logs as Fabric logs.

Cisco IOS logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Cisco IOS Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp

Cisco IOS Log Field	Normalized Fabric Log Field
appName	app_name
procName	app_proc
destName	dst_geo
destIntfName,intfName	dst_intf
destIpAddr	dst_ip
destMACAddr	dst_mac
destIpPort	dst_port
eventAction	event_action
msg_body	event_message
msg	event_ref
event_severity,eventSeverity	event_severity
ios_mode	event_subtype
eventType	event_type
phEventCategory	event_cat
hostIpAddr,reptDevIpAddr	host_ip
hostMACAddr	host_mac
hostName,hostIpAddr,reptDevIpAddr	host_name
ipProto	net_proto
recvPkts64	net_rcvdpkts
recvBytes64	net_recvbytes
sentBytes64	net_sentbytes
srcIntfName	src_intf
srcIpAddr	src_ip
srcMACAddr,srcMacAddr	src_mac
srcIpPort	src_port
userGrp	user_group
user	user_name

Cisco Meraki Firewall logs

FortiAnalyzer supports normalizing Cisco Meraki Firewall logs as Fabric logs.

Cisco Meraki Firewall logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Cisco Meraki Firewall Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
dstIpAddr	dst_ip
destMACAddr	dst_mac
destIpPort,dstIpPort	dst_port
msg_body	event_message
msg	event_ref
alarm	event_severity
meraki_mode	event_subtype
eventType	event_type
ip_address	host_ip
hostMACAddr	host_mac
host_name	host_name
httpMethod	http_method
infoURL	http_url
ipProto	net_proto
durationMSec	net_sessionduration
srcIpAddr,arpSrcIpAddr,tmp_client_ip,ip_src	src_ip
srcMACAddr	src_mac
srcIpPort	src_port

Cisco NX-OS logs

FortiAnalyzer supports normalizing Cisco NX-OS logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Cisco NX-OS syslogs and normalize core switch event by extracting device/source IP, interface names, user and source address details, and mapping NX-OS message codes into event_ref, severity, outcome, and action fields for SIEM analytics.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Cisco NX-OS Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
intfName	dst_intf
eventAction	event_action
msg_body	event_message
eventOutcome	event_outcome
eventRef	event_ref
eventSeverity	event_severity
nxos_mode	event_subtype
eventType	event_type
hostIpAddr,reptDevIpAddr	host_ip
hostMACAddr	host_mac
hostName	host_name
srcIpAddr	src_ip
src_port	src_port
user	user_name

Claroty Platform logs

FortiAnalyzer supports normalizing Claroty Platform logs as Fabric logs.

This log parser normalizes Claroty logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Claroty Platform Log Field	Normalized Fabric Log Field
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_name	app_name
app_version	app_ver
destName	dst_geo
destIpAddr	dst_ip
destMACAddr	dst_mac
event_cat	event_cat
msg_body	event_message
rule_name	event_outcome
status	event_profile
msg	event_ref
event_severity	event_severity
categoryType	event_subtype
eventType	event_type
hostIpAddr	host_ip
reptDevName	host_name
infoURL	http_url
siteName	src_domain
intfName,srcNetwork	src_intf
srcIpAddr	src_ip
srcMACAddr	src_mac
vulnCVEId,alertIdStr	threat_id
threatScore	threat_score
severity	threat_severity
alertCategory	threat_type
user	user_name
siteName,siteId	user_org

Clavister Firewall logs

FortiAnalyzer supports normalizing Clavister Firewall logs as Fabric logs.

This log parser normalizes Clavister firewall logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Clavister Firewall Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
destIntfName	dst_intf
destIpAddr	dst_ip
preNATDestIpAddr	dst_natip
preNATDestIpPort	dst_natport
destIpPort	dst_port
fwAction	event_action
logID	event_id
msg_body	event_message
fwRule	event_policy
shutdownReason	event_profile
eventSeverity	event_severity
log_type	event_subtype
eventType	event_type
ipProto	net_proto
durationMSec	net_sessionduration
sessionId	net_sessionid
srcIntfName	src_intf
srcIpAddr	src_ip
postNATSrcIpAddr	src_natip
postNATSrcIpPort	src_natport
srcIpPort	src_port

CrowdStrike Falcon logs

FortiAnalyzer supports normalizing CrowdStrike Falcon logs as Fabric logs.

CrowdStrike Falcon platform provides the endpoint detection and response (EDR) applications and techniques.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

CrowdStrike Falcon Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
procName	app_proc
destDomain	dst_domain
destIpAddr	dst_ip
destIpPort	dst_port
msg	event_message
event_outcome	event_outcome
event_severity	event_severity
event_subtype	event_subtype
eventType	event_type
device_category	event_cat
hashCode	file_hash
fileName,destFileName	file_name
filePath,destFilePath	file_path
device_vendor	host_hwvendor
hostIpAddr	host_ip
destName,srcName	host_name
http_url	http_url
srcDomain	src_domain
srcIpAddr	src_ip

CrowdStrike Falcon Log Field	Normalized Fabric Log Field
srcIpPort	src_port
destUser,srcUser,user	user_name

Dragos Platform logs

FortiAnalyzer supports normalizing Dragos Platform logs as Fabric logs.

Dragos platform logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Dragos Platform Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
ruleId	app_id
destDomain,destName	dst_domain
destIpAddr	dst_ip
destMACAddr	dst_mac
msg_body	event_message
msg	event_ref
eventSeverity	event_severity
type,subtype	event_subtype
eventType	event_type
hostIpAddr	host_ip
hostMACAddr	host_mac
hostName	host_name
srcDomain,srcName	src_domain
srcIpAddr	src_ip
srcMACAddr	src_mac
attackTechniqueId	threat_id

Dragos Platform Log Field	Normalized Fabric Log Field
attackTactic	threat_name

F5 Network logs

FortiAnalyzer supports normalizing F5 Network logs as Fabric logs.

F5 network logs provide insights into traffic management, system performance, security events, and configuration changes.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

F5 Network Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,dtime	data_timestamp
appName,ruleName	app_name
msg	event_message
responseCode	event_outcome
ruleName	event_policy
eventSeverity	event_severity
eventType	event_type
reptDevIpAddr	host_ip
reptDevName	host_name
httpMethod	http_method
httpUserAgent	http_useragent
recvBytes64	net_recvbytes
sentBytes64	net_sentbytes
srcIpAddr	src_ip
srcIpPort	src_port

Forcepoint Firewall logs

FortiAnalyzer supports normalizing Forcepoint Firewall logs as Fabric logs.

This log parser normalizes Forcepoint NGFW logs sent as CEF format, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Forcepoint Firewall Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_cat	app_cat
app_name	app_name
appTransportProto	app_proc
domain	dst_domain
destIntfName	dst_intf
destIpAddr	dst_ip
destMACAddr	dst_mac
destIpPort	dst_port
fwAction	event_action
msg_body	event_message
eventSeverity	event_severity
eventType	event_type
devEventTypeGrp	event_cat
reptIpAddr	host_ip
reptDevName	host_name
httpMethod	http_method
infoURL	http_url
ipProto	net_proto
recvBytes64	net_recvbytes

Forcepoint Firewall Log Field	Normalized Fabric Log Field
sentBytes64	net_sentbytes
srcIntfName	src_intf
srcIpAddr	src_ip
srcMACAddr	src_mac
srcIpPort	src_port

FortiNDR Cloud logs

FortiAnalyzer supports normalizing FortiNDR Cloud logs as Fabric logs.

This log parser enables FortiAnalyzer to parse FortiNDR Cloud detection logs and normalize alert events by extracting device, account, rule, indicator, timestamp, severity, confidence, and ATT&CK reference details for SIEM analytics.

Requirement:

- FortiAnalyzer 8.0.0 or later

The following field mapping applies:

FortiNDR Cloud Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
msg_tag	data_sourcetags
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_name	app_name
cloud_username	cloud_username
dst_geo_city	dst_geo_city
dst_geo_country	dst_geo_country
dst_ip	dst_ip
dst_port	dst_port
event_action	event_action
event_cat	event_cat
event_count	event_count
event_creation_time	event_creation_time

FortiNDR Cloud Log Field	Normalized Fabric Log Field
event_message	event_message
event_name	event_name
event_first_seen_time	event_first_seen_time
event_last_seen_time	event_last_seen_time
event_policy	event_policy
event_policyid	event_policyid
event_profile	event_profile
msg	event_rawmsg
event_severity	event_severity
event_source,sensor_id	event_source
event_status	event_status
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
host_ip	host_ip
host_name	host_name
http_method	http_method
http_status_code	http_status_code
http_status_message	http_status_message
http_host	http_host
http_url	http_url
http_useragent	http_useragent
http_request_bytes	http_request_bytes
http_response_bytes	http_response_bytes
net_direction	net_direction
net_proto	net_proto
net_sessionid	net_sessionid
src_geo_city	src_geo_city
src_geo_country	src_geo_country

FortiNDR Cloud Log Field	Normalized Fabric Log Field
src_ip	src_ip
src_port	src_port
threat_category	threat_category
threat_direction	threat_direction
threat_name	threat_name
threat_pattern	threat_pattern
threat_ref	threat_ref
threat_severity	threat_severity
threat_type	threat_type
user_id	user_id
user_name	user_name

Generic CEF logs

FortiAnalyzer supports normalizing Generic CEF logs as Fabric logs.

This log parser normalizes Generic CEF logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Generic CEF Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
cef_version	data_sourceversion
data_timestamp	data_timestamp
device_product	app_cat
app_name	app_name
appTransportProto,procName	app_proc
serviceName	app_service
app_version	app_ver

Generic CEF Log Field	Normalized Fabric Log Field
destDomain	dst_domain
destName	dst_geo
destIntfName	dst_intf
dst_ip,destIpAddr	dst_ip
destMACAddr	dst_mac
dst_natip,postNATDestIpAddr	dst_natip
postNATDestIpPort,preNATDestIpPort	dst_natport
destIpPort	dst_port
event_action,srcAction	event_action
msg_body,cef_body	event_message
errReason	event_outcome
extEventId	event_profile
msg	event_ref
event_severity	event_severity
eventType	event_type
cat_type,phEventCategory	event_cat
fileModificationTime	file_accessetime
fileType	file_ext
hashCode	file_hash
fileName	file_name
filePath	file_path
fileSize	file_size
device_vendor	host_hwvendor
host_ip	host_ip
hostMACAddr	host_mac
host_name,hostName	host_name
deviceIdentification	host_uid
httpCookie	http_cookie
httpMethod	http_method
httpReferrer	http_referer

Generic CEF Log Field	Normalized Fabric Log Field
infoURL	http_url
httpUserAgent	http_useragent
direction	net_direction
net_proto,tunnelProtocol	net_proto
totPkts64	net_rcvdpkts
recvBytes64,recvBytes	net_recvbytes
sentBytes64,sentBytes	net_sentbytes
durationMSec	net_sessionduration
sessionId	net_sessionid
srcDomain	src_domain
srcIntfName	src_intf
src_ip,srcIpAddr	src_ip
srcMACAddr	src_mac
src_natip,postNATSrcIpAddr	src_natip
postNATSrcIpPort	src_natport
srcIpPort	src_port
user_domain	user_domain
srcUserPriv	user_group
srcUserId	user_id
user_name,srcUser	user_name

Genuscreen Firewall logs

FortiAnalyzer supports normalizing Genuscreen Firewall logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Genuscreen syslog-delivered firewall logs and normalize network traffic events by extracting timestamps, source and destination addresses, ports, protocol, event pliocy details for SIEM analytics.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Genuscreen Firewall Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_service	app_service
dst_ip	dst_ip
dst_port	dst_port
event_action	event_action
event_id	event_id
msg_body	event_message
event_outcome	event_outcome
event_policy	event_policy
event_tags	event_tags
event_type	event_type
net_direction	net_direction
net_proto	net_proto
process_name	process_name
process_guid	process_guid
process_id	process_id
src_intf	src_intf
src_ip	src_ip
src_port	src_port

GitHub logs

FortiAnalyzer supports normalizing GitHub logs as Fabric logs.

GitHub audit and security logs provide visibility into user activity, repository changes, authentication events, and administrative actions. This log parser normalizes these logs when sent as syslog.

Requirement:

- FortiAnalyzer 7.6.3 or later

The following field mapping applies:

GitHub Log Field	Normalized Fabric Log Field
devid	data_sourceid
reptDevName	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
appName	app_name
appTransportProto	app_proc
destIpAddr	dst_ip
destIpPort	dst_port
actionName	event_action
errorString	event_error
message	event_message
msg_body	event_rawmsg
eventSeverity	event_severity
mode	event_source
event_tags	event_tags
event_type	event_type
activityType	event_cat
fileName	file_name
filePath	file_path
hostName,reptDevName	host_name
httpMethod	http_method
httpVersion	http_version
http_url,infoURL	http_url
http_useragent,httpUserAgent	http_useragent
recvPkts64	net_rcvdpkts
durationMSec	net_sessionduration
procId	process_id
srcIpAddr	src_ip
srcIpPort	src_port
user_email	user_email

GitHub Log Field	Normalized Fabric Log Field
userId	user_id
user	user_name

GitLab logs

FortiAnalyzer supports normalizing GitLab logs as Fabric logs.

This log parser allows FortiAnalyzer to normalize GitLab logs received as syslog messages using pattern matching.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

GitLab Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
event_action	event_action
log_json,log_str,log_msg	event_message
event_profile	event_profile
event_ref	event_ref
event_severity	event_severity
event_subtype	event_subtype
event_type	event_type
file_path	file_path
host_ip	host_ip
host_name	host_name
http_method	http_method
http_url	http_url
src_ip	src_ip
user_id	user_id
user_name	user_name

Google Cloud PubSub logs

FortiAnalyzer supports normalizing Google Cloud PubSub logs as Fabric logs.

Google Cloud Pub/Sub delivers messaging service logs for publishing, subscription, and message delivery events.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Google Cloud PubSub Log Field	Normalized Fabric Log Field
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
devid	data_sourceuuid
data_timestamp,dtime	data_timestamp
event_id	event_id
event_message	event_message
msg	event_rawmsg
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor

Indegy Security Platform logs

FortiAnalyzer supports normalizing Indegy Security Platform logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Indegy OT security CEF logs, and normalize OT network fields into SIEM data.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Indegy Security Platform Log Field	Normalized Fabric Log Field
data_timestamp,dtime	data_timestamp
data_version	data_version

Indegy Security Platform Log Field	Normalized Fabric Log Field
dst_ip	dst_ip
dst_mac	dst_mac
dst_port	dst_port
event_cat	event_cat
event_message	event_message
event_name	event_name
msg_body	event_rawmsg
event_severity	event_severity
event_source	event_source
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
host_ip	host_ip
src_ip	src_ip
src_mac	src_mac
src_port	src_port
user_id	user_id

ISC BIND DNS logs

FortiAnalyzer supports normalizing ISC BIND DNS logs as Fabric logs.

This log parser enables FortiAnalyzer to parse ISC BIND 9 DNS syslogs and normalize DNS query/response activity into SIEM fields such as source/client, queried domain, record type/class, and server details. It also categorizes common DNS conditions (e.g., refused/failed queries and update events) via event tags plus severity/action mapping.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

ISC BIND DNS Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype

ISC BIND DNS Log Field	Normalized Fabric Log Field
data_timestamp	data_timestamp
dns_query	dns_query
dns_querytype	dns_querytype
dns_query_class	dns_query_class
dns_response	dns_response
domainEntropy	dst_domain
destName	dst_geo
dst_ip	dst_ip
event_action,eventAction	event_action
msg_body	event_message
eventSeverity	event_severity
tmp_type	event_subtype
event_tags	event_tags
event_type	event_type
host_ip	host_ip
host_name	host_name
src_ip	src_ip

Juniper Firewalls logs

FortiAnalyzer supports normalizing Juniper Firewalls logs as Fabric logs.

Juniper SRX logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Juniper Firewalls Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp

Juniper Firewalls Log Field	Normalized Fabric Log Field
appTransportProto	app_proc
destIntfName	dst_intf
destIpAddr	dst_ip
destIpPort	dst_port
fwAction	event_action
msg_body	event_message
eventSeverity	event_severity
eventType	event_type
host_ip	host_ip
host_name	host_name
httpMethod	http_method
ipProto	net_proto
recvBytes64	net_recvbytes
sentBytes64	net_sentbytes
srcIntfName	src_intf
srcIpAddr	src_ip
srcIpPort	src_port
user	user_name

Kaspersky Security Center logs

FortiAnalyzer supports normalizing Kaspersky Security Center logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Kaspersky Security Center CEF-formatted syslog logs, extract key event attributes including source/destination, user, file path, and timestamp, and map vendor severity into normalized event severity for SIEM correlation and reporting.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Kaspersky Security Center Log Field	Normalized Fabric Log Field
data_timestamp	data_timestamp

Kaspersky Security Center Log Field	Normalized Fabric Log Field
dst_ip	dst_ip
dst_port	dst_port
event_action	event_action
event_msg	event_message
cef_msg_body	event_rawmsg
event_severity	event_severity
cef_tag	event_tags
cef_type	event_type
event_vendor	event_vendor
file_path	file_path
host_name	host_name
src_ip	src_ip
src_port	src_port
threat_name	threat_name
user	user_name

Linux Audit logs

FortiAnalyzer supports normalizing Linux Audit logs as Fabric logs.

This log parser normalizes Linux Audit logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Linux Audit Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
procName	app_proc
app_ref	app_ref
destName	dst_domain

Linux Audit Log Field	Normalized Fabric Log Field
eventAction	event_action
msgId	event_id
sub_msg,msg_body	event_message
event_outcome	event_outcome
msg	event_ref
eventSeverity	event_severity
eventType	event_type
fileType	file_ext
hashCode	file_hash
hostIpAddr	host_ip
hostMACAddr	host_mac
hostName	host_name
direction	net_direction
srcName	src_domain
userId	user_id
user	user_name

Linux DHCP logs

FortiAnalyzer supports normalizing Linux DHCP logs as Fabric logs.

This log parser normalizes Linux DHCP logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

Linux DHCP Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
destName	dst_geo
eventAction	event_action

Linux DHCP Log Field	Normalized Fabric Log Field
msg_body	event_message
eventSeverity	event_severity
eventType	event_type
hostIpAddr	host_ip
hostMACAddr	host_mac
hostName	host_name

McAfee Anti-Virus logs

FortiAnalyzer supports normalizing McAfee Anti-Virus logs as Fabric logs.

This log parser normalizes McAfee Anti-Virus logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

McAfee Anti-Virus Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
extEventRecvProto	app_cat
appName	app_name
procName	app_proc
appVersion	app_ver
domain	dst_domain
destName	dst_geo
destIpAddr	dst_ip
destIpPort	dst_port
msg_body	event_message
ruleName	event_profile
eventSeverity	event_severity

McAfee Anti-Virus Log Field	Normalized Fabric Log Field
eventType	event_type
fileName	file_name
hostIpAddr	host_ip
hostLocation	host_location
hostMACAddr	host_mac
hostName	host_name
osType	host_osfamily
osVersion	host_osver
machineGUID	host_uid
infoURL	http_url
senderMailAddr	mail_from
mailSubject	mail_subject
receiverMailAddr	mail_to
srcIpAddr	src_ip
threatLevel	threat_severity
threatCategory	threat_type
user	user_name

McAfee Firewall Syslog logs

FortiAnalyzer supports normalizing McAfee Firewall Syslog logs as Fabric logs.

This log parser normalizes McAfee firewall syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

McAfee Firewall Syslog Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp

McAfee Firewall Syslog Log Field	Normalized Fabric Log Field
appName	app_name
processId	app_proc
logId	app_ref
destFwZone	dst_domain
destIpAddr	dst_ip
destIpPort	dst_port
msg_body	event_message
fwRule	event_policy
msg	event_ref
eventSeverity	event_severity
eventType	event_type
host_ip	host_ip
host_name,hostName	host_name
ipProto	net_proto
ipConnId	net_sessionid
srcFwZone	src_domain
hostLocation	src_geo
srcIpAddr	src_ip
srcIpPort	src_port
threatCategory	threat_name
threatLevel	threat_severity

McAfee Web Gateway logs

FortiAnalyzer supports normalizing McAfee Web Gateway logs as Fabric logs.

The following field mapping applies:

McAfee Web Gateway Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
data_sourcetype	data_sourcetype
data_sourceversion	data_sourceversion

McAfee Web Gateway Log Field	Normalized Fabric Log Field
data_timestamp,itime	data_timestamp
app_name	app_name
app_ver	app_ver
dst_domain	dst_domain
dst_ip	dst_ip
event_action	event_action
event_cat	event_cat
event_error	event_error
event_id	event_id
event_policy	event_policy
msg_body	event_rawmsg
event_severity	event_severity
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
file_ext	file_ext
host_name	host_name
http_method	http_method
http_status_code	http_status_code
http_url	http_url
http_useragent	http_useragent
http_version	http_version
net_sentbytes	net_sentbytes
src_ip	src_ip
threat_name	threat_name
threat_type	threat_type
user_name	user_name

Microsoft 365 Defender logs

FortiAnalyzer supports normalizing Microsoft 365 Defender logs as Fabric logs.

This log parser allows FortiAnalyzer to normalize Microsoft 365 Defender logs in JSON format received using the Microsoft 365 Defender Connector's data ingestion option.

Requirement:

- FortiAnalyzer 7.6.3 or later

The following field mapping applies:

Microsoft 365 Defender Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourceuuid	data_sourceuuid
data_sourcetags	data_sourcetags
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,event_creation_time	data_timestamp
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
event_cat	event_cat
event_creation_time	event_creation_time
event_first_seen_time	event_first_seen_time
event_id	event_id
event_last_seen_time	event_last_seen_time
event_message	event_message
event_name	event_name
event_outcome	event_outcome
incident_name	event_profile
msg	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_source	event_source
event_status	event_status

Microsoft 365 Defender Log Field	Normalized Fabric Log Field
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
file_hash	file_hash
file_name	file_name
file_path	file_path
host_name	host_name
host_osfamily	host_osfamily
host_uid	host_uid
process_command_line	process_command_line
process_id	process_id
process_parent_name	process_parent_name
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
threat_action	threat_action
threat_category	threat_category
threat_id	threat_id
threat_message	threat_message
threat_ref	threat_ref
threat_severity	threat_severity
user_domain	user_domain
user_id	user_id
user_name	user_name

Microsoft CyberX logs

FortiAnalyzer supports normalizing Microsoft CyberX logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Microsoft CyberX (Defender for IoT) CEF logs, and normalize OT network fields into SIEM data.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Microsoft CyberX Log Field	Normalized Fabric Log Field
data_timestamp,dtime	data_timestamp
data_version	data_version
app_name	app_name
dst_ip	dst_ip
dst_mac	dst_mac
event_cat	event_cat
event_end_time	event_end_time
event_error	event_error
event_message	event_message
event_name	event_name
msg_body	event_rawmsg
event_severity	event_severity
event_source	event_source
event_start_time	event_start_time
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
src_ip	src_ip
src_mac	src_mac

Microsoft Entra ID logs

FortiAnalyzer supports normalizing Microsoft Entra ID logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Microsoft Entra ID (Azure AD) audit/sign-in logs and normalize identity and access events by extracting user, group, device, and application details (e.g., user principal, tenant, client IP, app/resource, conditional access context) and mapping Entra operation/result codes into SIEM fields such as event_type/event_subtype, event_ref, event_severity, event_outcome, and event_action for security analytics.

Requirement:

- FortiAnalyzer 7.6.2 or later

The following field mapping applies:

Microsoft Entra ID Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_action	app_action
app_name	app_name
app_service	app_service
event_action	event_action
event_cat	event_cat
event_creation_time	event_creation_time
event_error	event_error
event_error_code	event_error_code
event_message	event_message
event_name	event_name
event_outcome	event_outcome
msg	event_rawmsg
event_severity	event_severity
event_source	event_source
event_start_time	event_start_time
msg_tag	event_tags
event_type	event_type
host_name	host_name
host_osfamily	host_osfamily
host_type	host_type
host_uid	host_uid
http_useragent	http_useragent
logon_type	logon_type
logon_user_claims	logon_user_claims
src_geo_city	src_geo_city
src_geo_country	src_geo_country

Microsoft Entra ID Log Field	Normalized Fabric Log Field
src_geo_latitude	src_geo_latitude
src_geo_longitude	src_geo_longitude
src_geo_region	src_geo_region
src_ip	src_ip
threat_name	threat_name
threat_ref	threat_ref
threat_severity	threat_severity
threat_type	threat_type
user_id	user_id
user_name	user_name

Nessus logs

FortiAnalyzer supports normalizing Nessus logs as Fabric logs.

Tenable Nessus generates vulnerability scan logs containing host details, plugin IDs, CVEs, severities, and remediation information.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Nessus Log Field	Normalized Fabric Log Field
data_sourcenode	data_sourcenode
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
devid	data_sourceuuid
data_timestamp,dtime	data_timestamp
event_end_time	event_end_time
event_error	event_error
event_id	event_id
event_message	event_message
event_name	event_name

Nessus Log Field	Normalized Fabric Log Field
event_outcome	event_outcome
event_profile	event_profile
msg,msg_body	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_source	event_source
event_start_time	event_start_time
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
host_ip	host_ip
host_name	host_name
host_osfamily	host_osfamily
http_status_code	http_status_code
http_status_message	http_status_message
http_version	http_version
net_proto	net_proto
src_geo_city	src_geo_city
src_geo_country	src_geo_country
src_geo_region	src_geo_region
src_ip	src_ip
src_port	src_port
threat_cveid	threat_cveid
threat_message	threat_message
threat_name	threat_name
threat_score	threat_score
threat_severity	threat_severity
threat_type	threat_type
user_name	user_name
user_org	user_org

Nozomi Networks logs

FortiAnalyzer supports normalizing Nozomi Networks logs as Fabric logs.

This log parser normalizes Nozomi networks logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Nozomi Networks Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
appTransportProto,procName	app_proc
destIpAddr	dst_ip
destMACAddr	dst_mac
destIpPort	dst_port
msg_body	event_message
msg	event_ref
summary	event_subtype
eventType	event_type
reptDevName	host_name
srcIpAddr	src_ip
srcMACAddr	src_mac
srcIpPort	src_port
user	user_name

Office 365 Management Activity logs

FortiAnalyzer supports normalizing Office 365 Management Activity logs as Fabric logs.

This log parser allows FortiAnalyzer to parse and normalize information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra activity logs. Data can be ingested using the Microsoft Management Activity API Connector.

Requirement:

- FortiAnalyzer 7.6.2 or later

The following field mapping applies:

Office 365 Management Activity Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_sourceuuid	data_sourceuuid
event_creation_time	data_timestamp
app_action	app_action
app_id	app_id
app_name	app_name
app_ref	app_ref
app_ver	app_ver
event_action	event_action
event_creation_time	event_creation_time
event_error	event_error
event_error_code	event_error_code
event_id	event_id
event_message	event_message
event_name	event_name
event_policy	event_policy
event_profile	event_profile
msg	event_rawmsg
event_severity	event_severity
event_source	event_source
event_start_time	event_start_time
event_status	event_status
event_subtype	event_subtype
msg_tag	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor

Office 365 Management Activity Log Field	Normalized Fabric Log Field
file_ext	file_ext
file_hash	file_hash
file_name	file_name
file_path	file_path
host_ip	host_ip
host_name	host_name
host_osname	host_osname
host_type	host_type
http_url	http_url
http_useragent	http_useragent
logon_type	logon_type
logon_user_claims	logon_user_claims
mail_attachment	mail_attachment
mail_from	mail_from
mail_subject	mail_subject
mail_to	mail_to
net_direction	net_direction
process_name	process_name
src_ip	src_ip
threat_category	threat_category
threat_message	threat_message
threat_name	threat_name
threat_ref	threat_ref
threat_severity	threat_severity
threat_type	threat_type
user_authtype	user_authtype
user_classification	user_classification
user_domain	user_domain
user_id	user_id
user_name	user_name
user_org	user_org

Okta logs

FortiAnalyzer supports normalizing Okta logs as Fabric logs.

This log parser normalizes Okta logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.6.2 or later

The following field mapping applies:

Okta Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
data_version	data_version
event_action	event_action
event_creation_time	event_creation_time
event_message	event_message
event_name	event_name
event_outcome	event_outcome
msg_body	event_rawmsg
actorName	event_resource_group
actorId	event_resource_id
eventSeverity	event_severity
event_status	event_status
event_subtype	event_subtype
eventTag	event_tags
eventType	event_type
event_uuid	event_uuid
host_osname	host_osname
http_url	http_url
http_useragent	http_useragent
targetType	logon_type
targetUser	logon_user_claims

Okta Log Field	Normalized Fabric Log Field
targetName	logon_virtual_account
net_sessionid	net_sessionid
net_ssid	net_ssid
src_asset_id	src_asset_id
src_domain	src_domain
src_geo	src_geo
src_geo_city	src_geo_city
src_geo_country	src_geo_country
src_geo_country_code	src_geo_country_code
src_geo_latitude	src_geo_latitude
src_geo_longitude	src_geo_longitude
src_ip	src_ip
userType	user_authtype
user	user_name

Palo Alto Cortex XDR logs

FortiAnalyzer supports normalizing Palo Alto Cortex XDR logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Palo Alto Cortex XDR CEF syslogs, classify alert and audit events, then normalize key endpoint, user, process, file, and threat indicators into FAZ SIEM fields.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Palo Alto Cortex XDR Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
cef_tag	data_sourcetags
data_sourcetype	data_sourcetype
data_sourceversion,agent_version	data_sourceversion
data_timestamp,event_time	data_timestamp
app_proc	app_proc

Palo Alto Cortex XDR Log Field	Normalized Fabric Log Field
dvchost	dst_domain
event_act	event_action
event_end_time	event_end_time
event_error	event_error
event_msg	event_message
event_name	event_name
event_outcome	event_outcome
cef_msg_body	event_rawmsg
event_severity	event_severity
cef_product	event_source
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
event_cat	event_cat
file_hash	file_hash
file_name	file_name
file_path	file_path
src_host_name	host_name
request	http_url
net_proto	net_proto
process_name	process_name
process_parent_name	process_parent_name
process_command_line	process_command_line
src_ip	src_ip
attack_technique	threat_name
attack_tactic	threat_type
user_domain	user_domain
user_name	user_name
tenant_name	user_org

Palo Alto PAN-OS logs

FortiAnalyzer supports normalizing Palo Alto PAN-OS logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Palo Alto PAN-OS syslog CSV logs and normalize key network/session, policy, zone/interface, geo, and App-ID fields into FAZ SIEM data. It also enriches Threat events with URL/file extraction plus threat ID/name/category/severity mapping.

Requirement:

- FortiAnalyzer 7.6.2 or later

The following field mapping applies:

Palo Alto PAN-OS Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
app_cat	app_cat
keyword	app_data
app_name	app_name
app_proc,appPort	app_proc
app_ref	app_ref
id,type,name	app_risk
dst_zone	dst_domain
dst_geo_country	dst_geo_country
dst_intf	dst_intf
dst_ip	dst_ip
dst_natip	dst_natip
dst_natport	dst_natport
dst_port	dst_port
event_action	event_action
event_cat	event_cat
event_count	event_count
event_duration	event_duration
event_message	event_message
event_policy	event_policy

Palo Alto PAN-OS Log Field	Normalized Fabric Log Field
event_profile,errReason,profileName	event_profile
msg_body	event_rawmsg
event_ref	event_ref
event_severity	event_severity
fw_sn	event_source
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
file_name	file_name
objectPath	file_path
hostLocation	host_location
host_name,srcName	host_name
osName	host_osname
osVersion	host_osver
objType	host_type
uuid	host_uid
http_method	http_method
http_url	http_url
net_proto	net_proto
net_recvbytes	net_recvbytes
net_sentbytes	net_sentbytes
net_sentpkts	net_sentpkts
session_id	net_sessionid
src_zone	src_domain
src_geo_country	src_geo_country
src_intf	src_intf
src_ip,srcIpAddr	src_ip
src_natip	src_natip

Palo Alto PAN-OS Log Field	Normalized Fabric Log Field
src_natport	src_natport
src_port	src_port
threat_category	threat_category
threat_direction	threat_direction
threat_id	threat_id
threat_name	threat_name
threat_severity	threat_severity
threat_type	threat_type
user_domain	user_domain
userGrp	user_group
user_name,user	user_name

pfSense Firewall logs

FortiAnalyzer supports normalizing pfSense Firewall logs as Fabric logs.

This log parser enables FortiAnalyzer to parse pfSense syslog-delivered firewall logs and normalize network traffic events by extracting timestamps, source and destination addresses, ports, protocol, rule action, and service details for SIEM analytics.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

pfSense Firewall Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_service	app_service
dst_intf	dst_intf
dst_ip	dst_ip
dst_port	dst_port

pfSense Firewall Log Field	Normalized Fabric Log Field
event_action	event_action
event_id	event_id
msg_body,csv_msg_body	event_message
event_outcome	event_outcome
event_tags	event_tags
event_type	event_type
net_direction	net_direction
net_proto	net_proto
src_intf	src_intf
src_ip	src_ip
src_port	src_port

Proofpoint logs

FortiAnalyzer supports normalizing Proofpoint logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Proofpoint RFC5424 syslogs and normalize the logfmt-style message body into SIEM fields. It also classifies email and URL Defense message/click actions, and extracts rich threat metadata for email security analytics.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Proofpoint Log Field	Normalized Fabric Log Field
msg_id	data_sourcetags
version	data_sourceversion
data_timestamp	data_timestamp
app_name	app_name
dst_ip	dst_ip
event_action	event_action
event_cat	event_cat
event_creation_time	event_creation_time

Proofpoint Log Field	Normalized Fabric Log Field
event_message	event_message
event_name	event_name
event_policy	event_policy
event_profile	event_profile
msg_body	event_rawmsg
event_severity	event_severity
event_start_time	event_start_time
event_status	event_status
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
host_name	host_name
http_url	http_url
http_useragent	http_useragent
mail_from	mail_from
mail_messageid	mail_messageid
mail_size	mail_size
mail_subject	mail_subject
mail_to	mail_to
threat_category	threat_category
threat_id	threat_id
threat_name	threat_name
threat_pattern	threat_pattern
threat_ref	threat_ref
threat_type	threat_type

RSA SecurID logs

FortiAnalyzer supports normalizing RSA SecurID logs as Fabric logs.

RSA SecurID logs record authentication events, including successful logins, failed attempts, user lockouts, and system or agent status updates.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

RSA SecurID Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,dtime	data_timestamp
msg_body	event_message
event_outcome	event_outcome
event_policy	event_policy
event_severity	event_severity
event_type	event_type
event_cat	event_cat
host_ip	host_ip
host_name	host_name
net_sessionid	net_sessionid
host_ip	src_ip
user_name	user_name

SentinelOne logs

FortiAnalyzer supports normalizing SentinelOne logs as Fabric logs.

Parses SentinelOne platform logs sent as syslog. SentinelOne platform provides the endpoint detection and response (EDR) applications and techniques.

Requirement:

- FortiAnalyzer 7.4.2 or later

The following field mapping applies:

SentinelOne Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
appCategory	app_cat
procName	app_proc
destDomain	dst_domain
destName	dst_geo
destIpAddr	dst_ip
destIpPort	dst_port
event_id	event_id
msg	event_message
event_outcome	event_outcome
eventDesc	event_profile
eventSeverity,event_severity	event_severity
event_type	event_type
device_category	event_cat
hashCode	file_hash
fileName	file_name
filePath	file_path
device_vendor	host_hwvendor
hostIpAddr	host_ip
hostName,deviceIdentification	host_name
srcDomain	src_domain
srcIpAddr	src_ip
srcMACAddr	src_mac
srcIpPort	src_port
threatLevel	threat_severity
threatType	threat_type
groupName	user_group

SentinelOne Log Field	Normalized Fabric Log Field
accountId	user_id
srcUser,accountName	user_name

ServiceNow logs

FortiAnalyzer supports normalizing ServiceNow logs as Fabric logs.

ServiceNow generates incident, change, and service request logs, including ticket details, state transitions, priorities, and assignments.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

ServiceNow Log Field	Normalized Fabric Log Field
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
devid	data_sourceuuid
data_timestamp,dtime	data_timestamp
event_action	event_action
event_assignee	event_assignee
event_cat	event_cat
event_count	event_count
event_creation_time	event_creation_time
event_error	event_error
event_error_code	event_error_code
event_id	event_id
event_message	event_message
msg	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_source	event_source
event_status	event_status

ServiceNow Log Field	Normalized Fabric Log Field
event_status_code	event_status_code
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
incident_id	incident_id
user_domain	user_domain
user_id	user_id
user_name	user_name
user_org	user_org

SonicWall Firewalls logs

FortiAnalyzer supports normalizing SonicWall Firewalls logs as Fabric logs.

This log parser normalizes SonicWall logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

SonicWall Firewalls Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
appCategory	app_cat
appName	app_name
appTransportProto	app_proc
destName	dst_geo
destIntfName,intfName	dst_intf
destIpAddr	dst_ip
destMACAddr	dst_mac
destNatIpAddr	dst_natip

SonicWall Firewalls Log Field	Normalized Fabric Log Field
destNatIpPort	dst_natport
destIpPort	dst_port
fwAction	event_action
msg_body	event_message
type	event_outcome
fwRule	event_policy
eventSeverity	event_severity
eventType	event_type
event_cat	event_cat
host_ip	host_ip
reptDevName	host_name
httpMethod	http_method
mailFrom	mail_from
mailTo	mail_to
ipProto	net_proto
recvPkts64	net_rcvdpkts
recvBytes64	net_recvbytes
sentBytes64	net_sentbytes
srcIntfName	src_intf
srcIpAddr	src_ip
srcMACAddr	src_mac
srcNatIpAddr	src_natip
srcNatIpPort	src_natport
srcIpPort	src_port
user	user_name

Sophos Firewall logs

FortiAnalyzer supports normalizing Sophos Firewall logs as Fabric logs.

This log parser normalizes Sophos XGS logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Sophos Firewall Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
appCategory	app_cat
appName	app_name
appTransportProto	app_proc
destName	dst_geo
destIntfName,intfName	dst_intf
destIpAddr	dst_ip
destMACAddr	dst_mac
destIpPort	dst_port
fwAction	event_action
msg_body	event_message
newStatus	event_outcome
fwRule	event_policy
msg	event_ref
eventSeverity	event_severity
eventType	event_type
event_cat	event_cat
hostMACAddr	host_mac
reptDevName	host_name
httpMethod	http_method
infoURL	http_url
ipProto	net_proto
recvPkts64	net_rcvdpkts
recvBytes64	net_recvbytes
sentBytes64	net_sentbytes
durationMSec	net_sessionduration

Sophos Firewall Log Field	Normalized Fabric Log Field
srcIntfName	src_intf
srcIpAddr	src_ip
srcMACAddr	src_mac
srcIpPort	src_port
riskName	threat_name
userGroup	user_group
user	user_id
userName	user_name

Splunk logs

FortiAnalyzer supports normalizing Splunk logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Splunk API-delivered internal logs and normalize supervisor and sidecar events by extracting timestamps, host, service, process, URI, severity, and reference details for SIEM analytics.

Requirement:

- FortiAnalyzer 7.6.6 or later

The following field mapping applies:

Splunk Log Field	Normalized Fabric Log Field
msg_tag	data_sourcetags
data_timestamp	data_timestamp
app_service	app_service
event_cat	event_cat
event_message	event_message
msg	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_source	event_source
event_status	event_status
event_tags	event_tags

Splunk Log Field	Normalized Fabric Log Field
event_type	event_type
file_name	file_name
file_path	file_path
host_name	host_name
http_url	http_url
process_guid	process_guid
process_id	process_id
process_name	process_name

Stormshield Firewall logs

FortiAnalyzer supports normalizing Stormshield Firewall logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Stormshield firewall CEF syslogs, and normalize security and traffic fields into SIEM data.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Stormshield Firewall Log Field	Normalized Fabric Log Field
data_sourcetype	data_sourcetype
data_sourceuuid	data_sourceuuid
data_timestamp,dtime	data_timestamp
app_name	app_name
dst_domain	dst_domain
dst_geo_country	dst_geo_country
dst_geo_region	dst_geo_region
dst_intf	dst_intf
dst_intf_role	dst_intf_role
dst_ip	dst_ip
dst_mac	dst_mac
dst_natip	dst_natip

Stormshield Firewall Log Field	Normalized Fabric Log Field
dst_natport	dst_natport
dst_port	dst_port
event_action	event_action
event_cat	event_cat
event_count	event_count
event_duration	event_duration
event_message	event_message
event_policy	event_policy
event_policyid	event_policyid
event_policytype	event_policytype
msg_body	event_rawmsg
event_severity	event_severity
event_source	event_source
event_status	event_status
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
host_ip	host_ip
host_mac	host_mac
host_name	host_name
net_proto	net_proto
net_recvbytes	net_recvbytes
net_sentbytes	net_sentbytes
net_sessionduration	net_sessionduration
src_domain	src_domain
src_geo_country	src_geo_country
src_geo_region	src_geo_region
src_intf	src_intf
src_intf_role	src_intf_role
src_ip	src_ip

Stormshield Firewall Log Field	Normalized Fabric Log Field
src_mac	src_mac
src_natip	src_natip
src_natport	src_natport
src_port	src_port
user_id	user_id

Symantec Endpoint Protection logs

FortiAnalyzer supports normalizing Symantec Endpoint Protection logs as Fabric logs.

This log parser enables FortiAnalyzer to parse Symantec Endpoint Protection syslog events, extract antivirus and CIDS intrusion details such as host, user, file, threat information, and normalize severity, outcome, and event tags for security analytics.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Symantec Endpoint Protection Log Field	Normalized Fabric Log Field
data_timestamp	data_timestamp
dst_ip	dst_ip
dst_port	dst_port
event_action	event_action
event_msg	event_message
event_outcome	event_outcome
msg_body	event_rawmsg
event_severity	event_severity
event_tags	event_tags
event_type	event_type
event_cat	event_cat
event_source	event_source
event_vendor	event_vendor
file_name	file_name

Symantec Endpoint Protection Log Field	Normalized Fabric Log Field
file_path	file_path
host_ip	host_ip
host_mac	host_mac
host_name	host_name
src_ip	src_ip
src_port	src_port
virus_name	threat_name
domain	user_domain
user	user_name

Trend Micro Apex Central logs

FortiAnalyzer supports normalizing Trend Micro Apex Central logs as Fabric logs.

Trend Micro Apex Central is a centralized management console for Trend Micro's security products, providing a single point for monitoring and managing security across the entire network. This log parser normalizes logs sent from the Trend Micro Apex Central management console.

Requirement:

- FortiAnalyzer 7.6.4 or later

The following field mapping applies:

Trend Micro Apex Central Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
host_info,data_sourcename	data_sourcename
log_tag	data_sourcetags
data_sourcetype	data_sourcetype
data_sourceuuid	data_sourceuuid
data_timestamp	data_timestamp
app_action	app_action
app_name	app_name
app_ver	app_ver
dst_port	dst_port

Trend Micro Apex Central Log Field	Normalized Fabric Log Field
event_action	event_action
event_error_code	event_error_code
event_message	event_message
event_name	event_name
event_policyid	event_policyid
msg_body	event_rawmsg
event_severity	event_severity
event_source	event_source
event_tags	event_tags
event_type	event_type
event_vendor	event_vendor
file_hash	file_hash
file_path	file_path
host_name	host_name
http_url	http_url
process_command_line	process_command_line
process_name	process_name
src_ip	src_ip
src_port	src_port
threat_name	threat_name

WatchGuard Firewall logs

FortiAnalyzer supports normalizing WatchGuard Firewall logs as Fabric logs.

WatchGuard Firebox appliances generate firewall, VPN, threat detection, and system logs in syslog format.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

WatchGuard Firewall Log Field	Normalized Fabric Log Field
devid	data_sourceid

WatchGuard Firewall Log Field	Normalized Fabric Log Field
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
destDomain	dst_domain
destIntfName	dst_intf
destIpAddr,serverIpAddr	dst_ip
targetHostMACAddr,destMACAddr	dst_mac
preNATDestIpPort	dst_natport
destIpPort	dst_port
event_action	event_action
msg_body	event_message
event_policy	event_policy
errorString	event_ref
eventSeverity	event_severity
eventType	event_type
fileName	file_name
hostIpAddr	host_ip
host_name,httpHost	host_name
ipProto	net_proto
srcIntfName	src_intf
srcIpAddr,hostIpAddr	src_ip
srcMACAddr	src_mac
postNATSrcIpAddr	src_natip
postNATSrcIpPort	src_natport
srcIpPort	src_port
userId	user_id
user	user_name

Westermo WeOS logs

FortiAnalyzer supports normalizing Westermo WeOS logs as Fabric logs.

This log parser enables FortiAnalyzer to parse WeOS RFC5424-style syslogs, extract core header fields, then normalize key access-control/authentication signals and audit records into FAZ SIEM fields.

Requirement:

- FortiAnalyzer 7.6.2 or later

The following field mapping applies:

Westermo WeOS Log Field	Normalized Fabric Log Field
data_timestamp	data_timestamp
app_name	app_name
dst_ip	dst_ip
dst_port	dst_port
event_action	event_action
event_cat	event_cat
event_error_code	event_error_code
event_id	event_id
event_message	event_message
event_name	event_name
event_outcome	event_outcome
msg_body	event_rawmsg
event_severity	event_severity
event_source	event_source
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
host_name	host_name
net_recvbytes	net_recvbytes
net_sentbytes	net_sentbytes
process_id	process_id
src_ip	src_ip
src_port	src_port
user_classification	user_classification
user_id	user_id
user_name	user_name

Zscaler Firewall logs

FortiAnalyzer supports normalizing Zscaler Firewall logs as Fabric logs.

This log parser normalizes Zscaler firewall logs sent as syslog, matching by patterns.

Requirement:

- FortiAnalyzer 7.4.3 or later

The following field mapping applies:

Zscaler Firewall Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
appclass	app_cat
appName	app_name
serviceName	app_service
appVersion	app_ver
destcountry	dst_geo
destIpAddr	dst_ip
preNATDestIpAddr	dst_natip
destIpPort	dst_port
fwAction	event_action
logID	event_id
msg_body	event_message
ruleName,policyName	event_policy
reason	event_profile
eventSeverity	event_severity
log_type	event_subtype
eventType	event_type
webCategory,categoryType	event_cat
classifier,fileExt	file_ext
hashMD5	file_hash
fileType	file_hashtype

Zscaler Firewall Log Field	Normalized Fabric Log Field
fileName	file_name
hostLocation	host_location
deviceIdentification,clientName	host_name
osType	host_osfamily
osVersion	host_osver
deviceOwner	host_owner
httpMethod	http_method
httpReferrer	http_referer
infoURL	http_url
httpUserAgent	http_useragent
ipProto	net_proto
recvBytes	net_recvbytes
sentBytes	net_sentbytes
durationMSec	net_sessionduration
srcIpAddr	src_ip
postNATSrcIpAddr	src_natip
srcIpPort	src_port
threatType,dlpEngineVer,virusName	threat_name
threatCategory,dlpCategory,virusFamily	threat_type
emailId	user_id
user	user_name

Event handlers and alert handlers

This section provides details about the event handlers and alert handlers added as part of the FortiAnalyzer Security Automation Service. The handlers include multiple predefined rules used to generate events according to logs. They will have a default status (enabled or disabled) which can be edited in the FortiAnalyzer GUI; you can edit the status for rules within the handlers as well. These handlers can also be cloned and customized for your environment, if needed.

In FortiAnalyzer 8.0, event handlers are renamed to "alert handlers".

For information about finding and, if needed, enabling the handlers within the FortiAnalyzer GUI, see theFortiAnalyzer Administration Guide for the appropriate version.

The topics in this section provide the following information about the handlers:

- Description
- Minimum required version
- Default status
- Rules

Application Domain MAC Violations

The Application Domain MAC Violations handler was introduced in the version 26.05003 content pack. This handler can be used in FortiAnalyzer 8.0.0 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects FortiOS Application Domain MAC (Mandatory Access Control) violations, where a process attempted an operation denied by its security domain policy. Covers pre-chroot phase violations, Linux capability violations, and resource/syscall ACL denials. These events can indicate potential privilege escalation attempts, misconfigurations, or malicious activity within the application domain.
Status	Enabled
Rules	• Pre-Chroot Access Violation • Linux Capability Violation • Resource ACL Denial

Armis Alert Detected

The Armis Alert Detected handler was introduced in the version 24.12001 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Armis Asset Intelligence Platform alert has been detected.
Status	Enabled
Rules	• Armis Alert Detected

Aruba OS-CX - User Account Activity

The Aruba OS-CX - User Account Activity handler was introduced in the version 24.04004 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors Aruba OS-CX Switch platform activities related to user account management, including the admin deleting users from or adding a new user to the switch.
Status	Disabled
Rules	• User Deleted • User Added

AWS - CloudTrail Lifecycle and Tampering

The AWS - CloudTrail Lifecycle and Tampering handler was introduced in the version 25.08008 content pack. This handler can be used in FortiAnalyzer 7.6.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects creation, modification, suspension, or deletion of CloudTrail trails and settings, indicating attempts to disrupt audit logging.

Option	Configuration
Status	Disabled
Rules	• AWS CloudTrail Log Deleted • AWS CloudTrail Log Suspended • AWS CloudTrail Log Setting Updated • AWS CloudTrail Log Created • AWS CloudTrail Important Changes

AWS - EC2 Security and Data Exposure

The AWS - EC2 Security and Data Exposure handler was introduced in the version 25.08008 content pack. This handler can be used in FortiAnalyzer 7.6.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors for potentially risky or malicious changes and activity within AWS EC2 that could lead to data exposure, unauthorized access, or persistence.
Status	Disabled
Rules	• AWS EC2 User Data Download • AWS EC2 Snapshot Attribute Modified • AWS EC2 Network Access Control List Created • AWS EC2 Network Access Control List Deleted • AWS EC2 Encryption Disabled • AWS Execution via System Manager

AWS - IAM Identity and Access Management

The AWS - IAM Identity and Access Management handler was introduced in the version 25.11002 content pack. This handler can be used in FortiAnalyzer 7.6.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors for critical IAM security events including root account usage, weak authentication practices, policy modifications, credential changes, and group membership alterations that could indicate privilege escalation or unauthorized access.
Status	Disabled
Rules	• AWS Management Console Root Login • AWS IAM Assume Role Policy Update • AWS IAM Brute Force of Assume Role Policy • AWS IAM MFA Device Deactivated • AWS IAM Password Recovery Requested • AWS IAM Group Created • AWS IAM Group Deleted • AWS IAM User Added to Group

AWS - Monitoring and Logging Assets

The AWS - Monitoring and Logging Assets handler was introduced in the version 25.11002 content pack. This handler can be used in FortiAnalyzer 7.6.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Identifies deletion or stoppage of CloudWatch alarms/logs, Config recorders, Flow Logs, or GuardDuty detectors that could reduce monitoring visibility.
Status	Disabled
Rules	• AWS CloudWatch Alarm Deleted • AWS CloudWatch Log Group Deleted • AWS CloudWatch Log Stream Deleted • AWS Configuration Recorder Stopped • AWS GuardDuty Detector Deleted • AWS EC2 Flow Log Deleted

AWS - Relational Database Service (RDS) Lifecycle

The AWS - Relational Database Service (RDS) Lifecycle handler was introduced in the version 25.12003 content pack. This handler can be used in FortiAnalyzer 7.6.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors for AWS RDS database lifecycle events including cluster/instance creation, deletion, and stopping that could indicate unauthorized resource provisioning, data destruction, or service disruption.
Status	Disabled
Rules	• AWS RDS Cluster Created • AWS RDS Cluster Deleted • AWS RDS Instance or Cluster Stopped

AWS - Web Application Protection

The AWS - Web Application Protection handler was introduced in the version 25.12003 content pack. This handler can be used in FortiAnalyzer 7.6.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors for deletion of AWS WAF Access Control Lists, rules, or rule groups that could expose web applications to attacks.
Status	Disabled
Rules	• AWS WAF Access Control List Deleted • AWS WAF Rule or Rule Group Deleted

Cisco - Meraki New Splash User

The Cisco - Meraki New Splash User handler was introduced in the version 24.02006 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Meraki detects when a new user registers on an SSID through the splash page.
Status	Disabled
Rules	• Meraki New Splash User

Data Exfiltration over Remote Services

The Data Exfiltration over Remote Services handler was introduced in the version 24.10004 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects potential data exfiltration with large data transfers (>= 200MB), as a single or multiple transfers, over high-risk remote services.
Status	Enabled
Rules	• Large Data Exfiltration Detected - 1GB • Moderate Data Exfiltration Detected - 200MB

Dragos - Unresolved Malicious Mail Attachment

The Dragos - Unresolved Malicious Mail Attachment handler was introduced in the version 24.05003 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects that host anti-virus or content inspection devices found a Spam/Malicious Mail Attachment but could not remediate it. The sender is sending to 5 or more distinct receiver mail addresses.
Status	Disabled
Rules	• Spam or Malicious Mail Attachment Found

Endpoint Threat Detection

The Endpoint Threat Detection handler was introduced in the version 26.03005 content pack. This handler can be used in FortiAnalyzer 7.6.4 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects endpoint security threats including high severity Host IPS exploit events, unremediated malware found, and unremediated spyware found.
Status	Disabled
Rules	• Malware found but not remediated • Spyware found but not remediated • Kaspersky Exploit Prevention Triggered • Kaspersky malware object not cured

FortiNDR Cloud Detections

The FortiNDR Cloud Detections handler was introduced in the version 26.04003 content pack. It has been updated in the following versions:

- 26.05003

This handler can be used in FortiAnalyzer 8.0.0 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects FortiNDR Cloud detection events for a host, split by severity tier: high, moderate, and low.
Status	Disabled
Rules	• FortiNDR Cloud: High Severity Detection Triggered For a Host • FortiNDR Cloud: Moderate Severity Detection Triggered For a Host • FortiNDR Cloud: Low Severity Detection Triggered For a Host

Group Membership Changes

The Group Membership Changes handler was introduced in the version 25.08008 content pack. This handler can be used in FortiAnalyzer 7.6.4 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors and detects changes to local Linux group memberships and administrative privileges, including; addition or removal of users from any group, changes to the sudoers file or other privilege-granting configurations.
Status	Disabled
Rules	• Linux User Deleted from Groups • Linux User Added to Groups • Linux User Deleted from Admin Groups • Linux User Added to Administrative Groups

High Volume DNS Traffic

The High Volume DNS Traffic handler was introduced in the version 24.03004 content pack. It has been updated in the following versions:

- 24.06001
- 24.07001
- 24.08001
- 24.11004
- 24.12002
- 25.04006

This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Identifies a situation where a host experiences an unusually high volume of DNS name resolution queries.
Status	Disabled
Rules	• High Volume of Denied DNS Queries • High Volume of DNS Requests From Single Host • High Volume DNS Queries To Same Domain

Option	Configuration
	• High Volume of Denied DNS Queries 1

ICS - Collection

The ICS - Collection handler was introduced in the version 25.04006 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0100 - Collection. Adversaries may gather data of interest and domain knowledge on your ICS environment to inform their goal.
Status	Disabled
Rules	• Man in the Middle • Automated Collection • Data from Information Repositories • Detect Operating Mode • IO Image • Monitor Process State • Point Tag Identification • Program Upload • Screen Capture

ICS - Command and Control

The ICS - Command and Control handler was introduced in the version 24.05003 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing Mitre ICS Tactic ID TA0101 - Command and Control. Adversaries may communicate with and control compromised systems to blend in with normal network traffic and avoid more detailed inspection.

Option	Configuration
Status	Disabled
Rules	• Standard Application Layer Protocol • Connection Proxy

ICS - Discovery

The ICS - Discovery handler was introduced in the version 25.03004 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0102 - Discovery. Adversaries may be locating information to gain knowledge about the ICS environment.
Status	Disabled
Rules	• Network Connection Enumeration • Network Sniffing • Remote System Discovery • Remote System Information Discovery • Wireless Sniffing

ICS - Evasion

The ICS - Evasion handler was introduced in the version 24.05003 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0103 - Evasion. Adversaries may be trying to avoid security defenses to evade detection.
Status	Disabled
Rules	• Indicator Removal on Host • Masquerading • Spoof Reporting Message

ICS - Execution

The ICS - Execution handler was introduced in the version 25.03004 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing Mitre ICS Tactic ID TA0104 - Execution. Adversaries may be trying to run code or manipulate system functions, parameters, and data in an unauthorized way.
Status	Disabled
Rules	• Change Operating Mode • Command-Line Interface • Execution through API • Graphical User Interface • Hooking • Native API • Scripting • User Execution

ICS - Exploitation for Evasion

The ICS - Exploitation for Evasion handler was introduced in the version 26.01002 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	An ICS monitoring system has detected an event containing MITRE ICS Technique ID T0820 - Exploitation for Evasion. Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to evade detection.
Status	Disabled
Rules	• Exploitation for Evasion

ICS - Impact

The ICS - Impact handler was introduced in the version 25.03004 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0105 - Impact. Adversaries may cause damage and destruction of ICS systems, data, and their surrounding environment.
Status	Disabled
Rules	• Damage to Property • Denial of Control • Denial of View • Loss of Availability • Loss of Control • Loss of Productivity and Revenue • Loss of Protection • Loss of Safety • Loss of View • Manipulation of Control • Manipulation of View • Theft of Operational Information

ICS - Impair Process Control

The ICS - Impair Process Control handler was introduced in the version 24.05003 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing Mitre ICS Tactic ID TA0106 - Impair Process Control. Adversaries may try to manipulate, disable, or damage a process function. The adversary may be able to generate instability on the process function associated with that particular point.
Status	Disabled
Rules	• Brute Force IO

Option	Configuration
	• Modify Parameter • Unauthorized Command Message

ICS - Inhibit Response Function

The ICS - Inhibit Response Function handler was introduced in the version 25.04006 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing Mitre ICS Tactic ID TA0107 - Inhibit Response Function. Adversaries may be hindering the safeguards put in place to prevent the safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
Status	Disabled
Rules	• Activate Firmware Update Mode • Alarm Suppression • Command Blocked • Block Reporting Message • Serial COM Blocked • Data Destruction • Denial of Service • Device Restart Shutdown • Manipulate IO Image • Modify Alarm Settings • Service Stop

ICS - Initial Access

The ICS - Initial Access handler was introduced in the version 25.03004 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0108 - InitialAccess. Adversaries may be trying to gain access to the ICS environment.
Status	Disabled
Rules	• Drive-by Compromise • Exploit Public-Facing Application • Exploitation of Remote Services • External Remote Services • Internet Accessible Device • Remote Services • Replication Through Removable Media • Rogue Master • Spearphishing Attachment • Supply Chain Compromise • Transient Cyber Asset • Wireless Compromise

ICS - Lateral Movement

The ICS - Lateral Movement handler was introduced in the version 25.04006 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0109 - Lateral Movement. Adversaries may leverage techniques to move through the ICS environment.
Status	Disabled
Rules	• Default Credentials • Lateral Tool Transfer • Program Download

ICS - Persistence

The ICS - Persistence handler was introduced in the version 25.04006 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0110 - Persistence. Adversaries may be trying to maintain their foothold in the ICS environment.
Status	Disabled
Rules	• Modify Program • Module Firmware • Project File Infection • System Firmware • Valid Accounts

ICS - Privilege Escalation

The ICS - Privilege Escalation handler was introduced in the version 25.04006 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	ICS monitor detecting an event containing MITRE ICS Tactic ID TA0111 - Privilege Escalation. Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.
Status	Disabled
Rules	• Exploitation for Privilege Escalation

ICS - Rootkit Found

The ICS - Rootkit Found handler was introduced in the version 26.01002 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	An ICS monitoring system has detected an event containing MITRE ICS Technique ID T0851 - Rootkit. Adversaries may deploy rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components.
Status	Enabled
Rules	• Rootkit Found

Indicators of Account Compromise

The Indicators of Account Compromise handler was introduced in the version 26.02002 content pack. This handler can be used in FortiAnalyzer 7.6.5 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors Office 365 and Microsoft Entra for account compromise indicators including anomalous login patterns, Microsoft Identity Protection risk detections, risky user identifications, and multi-factor authentication disablement. Combines data from Office 365 Management Activity API and Microsoft Entra Graph API for comprehensive threat detection.
Status	Disabled
Rules	• Microsoft Entra Identity Protection Risky User Identified • Office365 Abnormal Login Pattern Detected • Office365 Identity Protection Detected a Risky User or SignIn Activity • Office365 Strong Authentication Disabled for a User

Invalid TCP-UDP Port Traffic

The Invalid TCP-UDP Port Traffic handler was introduced in the version 24.06001 content pack. It has been updated in the following versions:

- 24.07001
- 24.08001
- 24.11004
- 24.12002
- 25.04006

This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Identifies unauthorized TCP/UDP traffic on port number 0, occurring more than 10 times within a 3-minute period.
Status	Disabled
Rules	• Multiple Invalid TCP or UDP Traffic • Multiple Invalid TCP or UDP Traffic 1

Linux - Suspicious System Events

The Linux - Suspicious System Events handler was introduced in the version 24.03004 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	This handler monitors Linux system events that are deemed suspicious and show potential threat in the endpoint device.
Status	Disabled
Rules	• Linux Buffer Overflow • Unusual Process Execution from Temp • Account Locked

Log4J Exploit Request Detected

The Log4J Exploit Request Detected handler was introduced in the version 24.11004 content pack. It has been updated in the following versions:

- 24.12002
- 25.02004
- 25.04006
- 26.05003

This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects Log4J Exploit Request via Regex by inspecting HTTP User Agent, URL, Referrer, Cookie for indicators of Log4J CVE-2021-44228 exploitation.
Status	Enabled
Rules	• Log4J Exploit Request Detected By Regex

Malicious Mail Activities

The Malicious Mail Activities handler was introduced in the version 24.07001 content pack. It has been updated in the following versions:

- 24.10004

This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects that host anti-virus or content inspection devices detected a spam/malicious mail activity.
Status	Disabled
Rules	• Spam or Malicious Mail Attachment found but not remediated

Multiple Logon Failures

The Multiple Logon Failures handler was introduced in the version 24.06001 content pack. It has been updated in the following versions:

- 24.07001
- 24.08001
- 24.12002
- 25.01009
- 25.02004
- 25.03004
- 25.04006
- 25.05005
- 25.06006

This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Identifies a single source repeatedly failing to log in.
Status	Disabled
Rules	• Multiple Logon Failures:From Same Src to Multiple Dest • Multiple Logon Failures:Same Src and Dest with Multiple Accounts • Multiple Logon Failures:From Same Src to Multiple Dest 1 • Multiple Logon Failures:Same Src and Dst with Multiple Acct. 1

Palo Alto Cortex XDR Alerts

The Palo Alto Cortex XDR Alerts handler was introduced in the version 26.05003 content pack. This handler can be used in FortiAnalyzer 7.6.4 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects alerts raised by Palo Alto Cortex XDR. Distinguishes between threats that were prevented (blocked) and threats that were only detected (not blocked). Detected alerts are escalated to a higher severity since the threat may still be active.
Status	Disabled
Rules	• Cortex XDR Alert Detected • Cortex XDR Alert Prevented

Phishing Attack Detected

The Phishing Attack Detected handler was introduced in the version 24.07001 content pack. This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Detects that host anti-virus or content inspection devices found phishing attacks.
Status	Disabled
Rules	• Phishing attack found but not remediated

Suspicious DHCP Traffic

The Suspicious DHCP Traffic handler was introduced in the version 24.03004 content pack. This handler can be used in FortiAnalyzer 7.4.2 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	This handler detects unusual activity in the DHCP traffic that may be indicative of an ongoing attack such as MAC Spoofing Attack, Rogue DHCP Server etc.
Status	Disabled
Rules	• DHCP Starvation (MAC Spoofing) Attack • High Volume of DHCP Release - Rogue DHCP Server

TCP DDoS Attack

The TCP DDoS Attack handler was introduced in the version 24.07001 content pack. It has been updated in the following versions:

- 24.08001
- 24.12002
- 25.04006

This handler can be used in FortiAnalyzer 7.4.3 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Identifies a high volume of half-open TCP connections, originating from various unique sources, all targeting the same host and port within a brief time frame. This pattern could suggest that the destination server is experiencing an attack.
Status	Disabled
Rules	• Half Open TCP DDOS Attack

User Account Lifecycle and Status Changes

The User Account Lifecycle and Status Changes handler was introduced in the version 25.08008 content pack. This handler can be used in FortiAnalyzer 7.6.4 and later.

See below for a brief summary of the handler:

Option	Configuration
Description	Monitors and detects changes to Linux user accounts including creation, deletion, renaming, password updates, account property modifications, and unlocking events. This handler helps track key lifecycle events and configuration changes that may indicate administrative activity, user onboarding or offboarding, or unauthorized modifications to user identities. It provides visibility into the full lifecycle of local Linux accounts to support compliance, auditing, and security monitoring objectives.
Status	Disabled
Rules	• Linux Account Unlocked • Linux User Deleted • Linux User Name Changed • Linux User Password Changed • Linux User Created • Linux User Account Properties Changed

Reports

This section provides details about the reports added from FortiGuard as part of the FortiAnalyzer Security Automation Service.

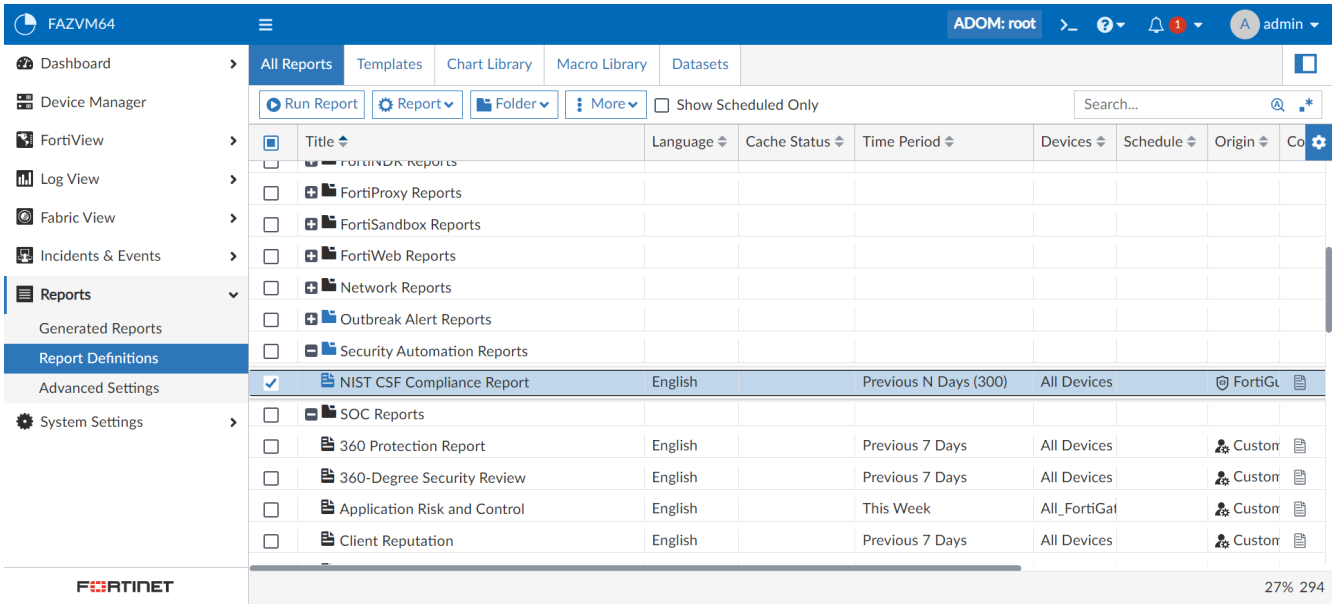
The reports can be found within the global *Security Automation Reports* folder in *Reports > Report Definitions > All Reports*. The charts and datasets used within the report are also added to the licensed FortiAnalyzer at the global level and named according to the report. An associated report template is not added.

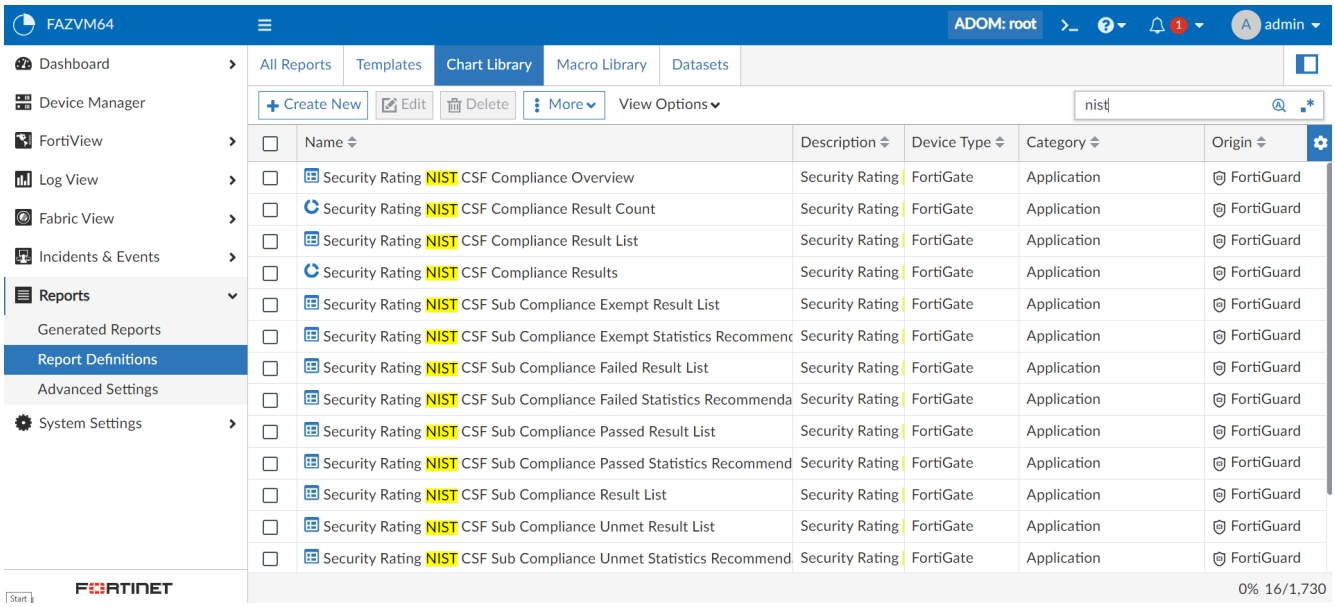
For compliance reports using standards from organizations such as the IEC, NIST, and PCI, the standards are included as metadata from FortiGuard and pushed to the FortiAnalyzer. This metadata is used to provide a compliance posture assessment against your security fabric, offering guidance on cybersecurity risk management best practices when applicable. In addition to the Security Automation Service license, these compliance reports also require a license for Security Rating Update (FGSA).

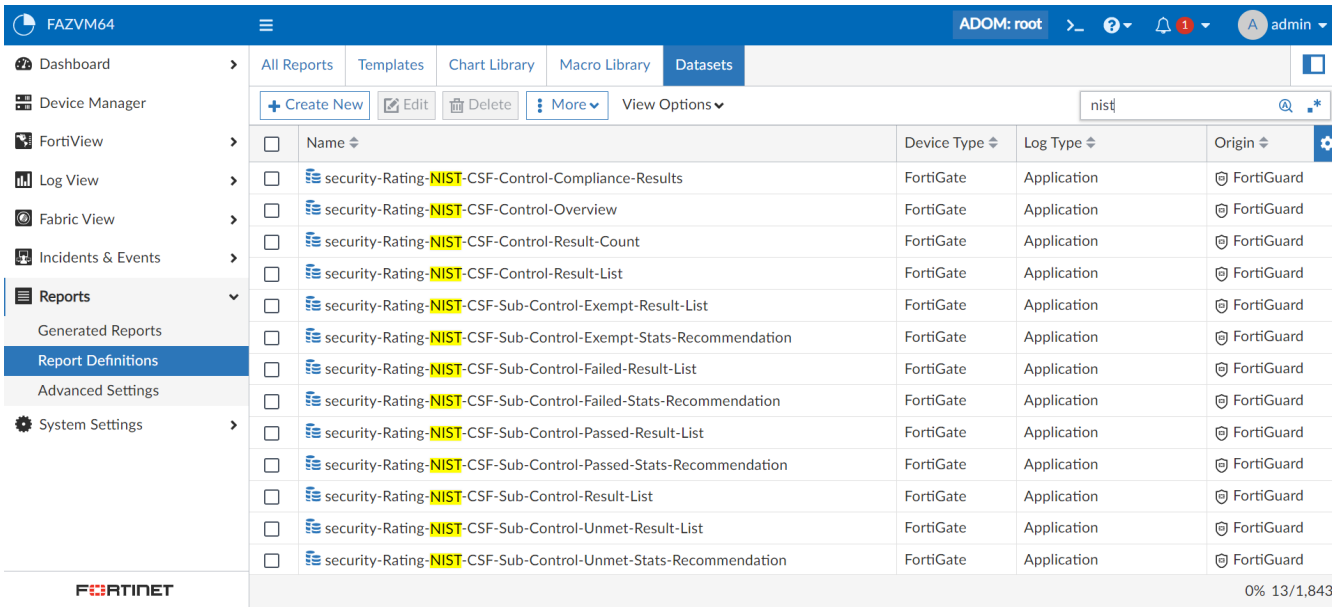
Example: NIST CSF Compliance Report

In this example, FortiGates in a security fabric are connected to the FortiAnalyzer. The FortiAnalyzer is licensed for the Security Automation Service and Security Rating Update, and it has access to the FortiGuard Distribution Server (FDS).

The *NIST CSF Compliance Report* configuration has been pushed from FortiGuard to FortiAnalyzer. The report, charts, and datasets are stored at the global level.







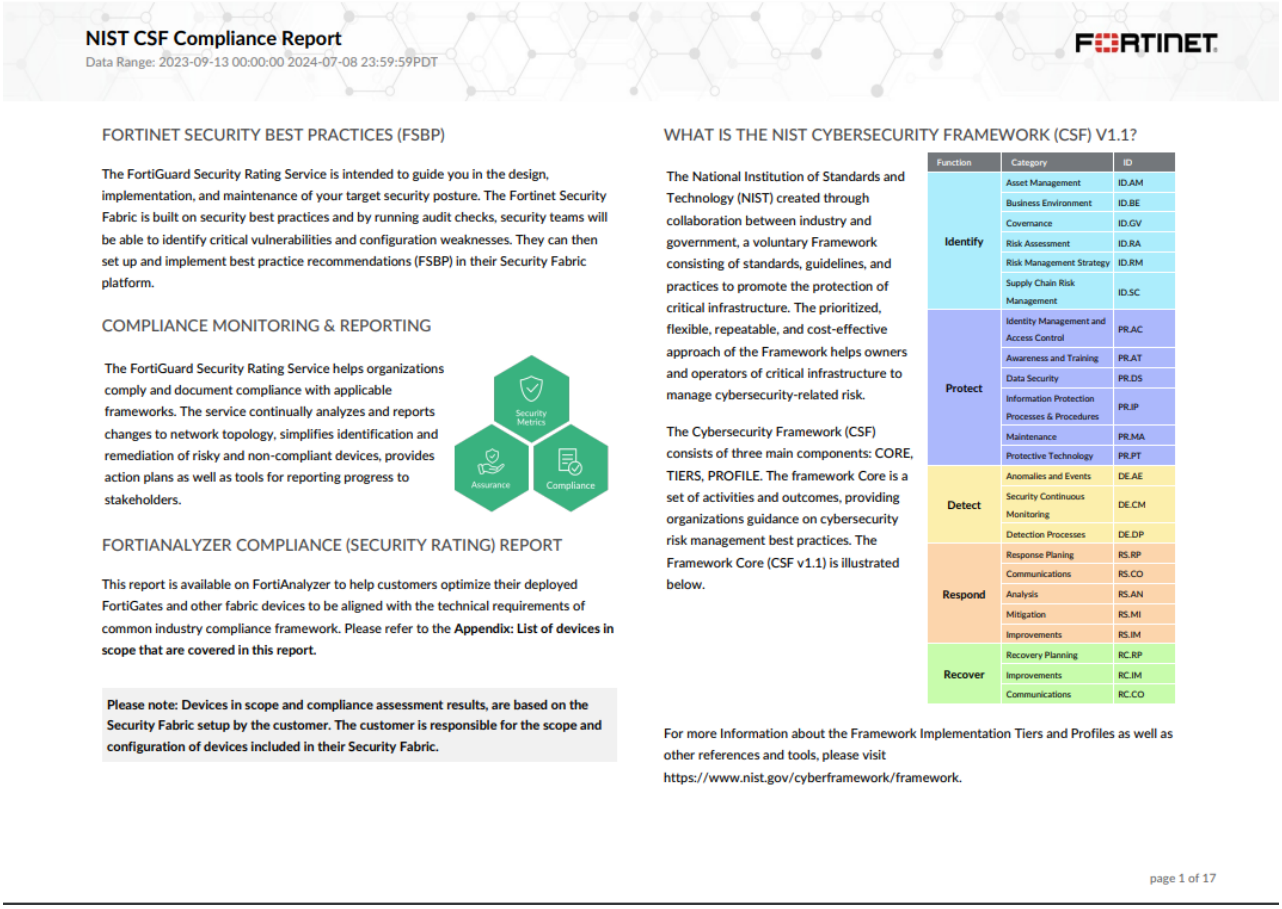
The data needed for generating this report are available in the FortiAnalyzer:

- Three Security Rating reports from have been received from the FortiGates
- The metatables (`security_nist_csf_fsbp_map` and `security_nist_csf_mdata`) have been received from FortiGuard

To run the report:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Select *NIST CSF Compliance Report*, and click *Run Report*.
3. Go to *Reports* > *Generated Reports* to view the status as the report is generated.
4. Once generated, in the *Format* column, click the format to open the report in.

Below is an excerpt example of the report generated in PDF format.



NIST CSF Compliance Report

Data Range: 2023-09-13 00:00:00 2024-07-08 23:59:59PDT

FORTINET

FORTINET SECURITY BEST PRACTICES (FSBP)

The FortiGuard Security Rating Service is intended to guide you in the design, implementation, and maintenance of your target security posture. The Fortinet Security Fabric is built on security best practices and by running audit checks, security teams will be able to identify critical vulnerabilities and configuration weaknesses. They can then set up and implement best practice recommendations (FSBP) in their Security Fabric platform.

COMPLIANCE MONITORING & REPORTING

The FortiGuard Security Rating Service helps organizations comply and document compliance with applicable frameworks. The service continually analyzes and reports changes to network topology, simplifies identification and remediation of risky and non-compliant devices, provides action plans as well as tools for reporting progress to stakeholders.

Security Metrics
Assurance
Compliance

FORTIANALYZER COMPLIANCE (SECURITY RATING) REPORT

This report is available on FortiAnalyzer to help customers optimize their deployed FortiGates and other fabric devices to be aligned with the technical requirements of common industry compliance framework. Please refer to the **Appendix: List of devices in scope that are covered in this report.**

Please note: Devices in scope and compliance assessment results, are based on the Security Fabric setup by the customer. The customer is responsible for the scope and configuration of devices included in their Security Fabric.

WHAT IS THE NIST CYBERSECURITY FRAMEWORK (CSF) V1.1?

The National Institution of Standards and Technology (NIST) created through collaboration between industry and government, a voluntary Framework consisting of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

The Cybersecurity Framework (CSF) consists of three main components: CORE, TIERS, PROFILE. The framework Core is a set of activities and outcomes, providing organizations guidance on cybersecurity risk management best practices. The Framework Core (CSF v1.1) is illustrated below.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planing	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

For more Information about the Framework Implementation Tiers and Profiles as well as other references and tools, please visit https://www.nist.gov/cyberframework/framework.

page 1 of 17

IEC 62443 report

The IEC 62443 report provides a security and compliance posture assessment of the customer's security fabric against IEC 62443.

This report is available as part of the version 25.01009 content pack. It has been updated in the following content pack versions:

- 25.08008
- 26.03005

This report can be used in FortiAnalyzer 7.4.3 and later.

NIST 800-53 report

The NIST 800-53 report provides a security and compliance posture assessment of the customer's security fabric against NIST SP800-53r5.

This report is available as part of version 24.11004 content pack. It has been updated in the following content pack versions:

- 25.08008
- 26.03005

This report can be used in FortiAnalyzer 7.4.3 and later.

NIST CSF Compliance report

The NIST CSF Compliance report provides a security and compliance posture assessment of the security fabric against NIST CSF v1.1.

This report is available as part of version 25.05003 content pack. In can be used in FortiAnalyzer 7.4.3 and later.It has been updated in the following content pack versions:

- 25.08008

This report can be used in FortiAnalyzer 7.4.3 and later.

PCI DSS v4.0.1 report

The PCI DSS v4.0.1 report provides a security and compliance posture assessment of the customer's Security Fabric implementation against the Payment Card Industry Data Security Standards (PCI DSS) version 4.0.1.

This report is available as part of the version 24.10004 content pack. It has been updated in the following content pack versions:

- 25.08008

This report can be used in FortiAnalyzer 7.4.3 and later.

Connectors and playbooks

This section provides details about the connectors and playbooks added as part of the FortiAnalyzer Security Automation Service. This includes the how to configure the connector as well as the available actions. Once configured, the connector actions can be used as part of playbooks in FortiAnalyzer.

Data ingestion actions

Some connectors include actions for data ingestion from a third-party service. For these connectors, you must enable the related log parser and configure a data ingestion schedule for the connector action. Once configured, a playbook will automatically be created to ingest logs; it will run according to the data ingestion schedule.

The related log parser will be assigned to a device in FortiAnalyzer to normalize the logs and insert them in the SIEM database (siemdb). This data ingestion device is automatically created once the first connector for data ingestion is configured. Rather than creating a new device for each connector, all subsequent log parsers used for data ingestion will also be automatically assigned to this device as well.

Once logs are ingested, you can view them in *Log View* > *Logs* > *All*. To quickly find logs ingested from a specific service, you can use the following text filter: `data_parsername="<log parser used for the data ingestion action>"`. The details about the related log parser are included when applicable for the connector action. For example, see the *Ingest Microsoft Management Activity API Logs* action described in Microsoft Management Activity API connector on page 141.

AWS CloudTrail connector

AWS CloudTrail enables auditing, security monitoring, and operational monitoring by logging your AWS account activity. The connector's data ingestion option allows to ingest the CloudTrail events into FortiAnalyzer. For more information, please refer to the AWS CloudTrail API Reference.

The AWS CloudTrail connector is available as part of version 25.07004 content pack. It has further version updates in the following content pack:

- 25.08008
- 25.09003
- 25.10004
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the AWS CloudTrail connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
aws_access_key	Enter the access key.
aws_iam_role	Enter the IAM role.
aws_region	Enter the region.
aws_secret_access_key	Enter the secret access key.
config_type	Select one of the following: • IAM Role • Access Credentials
verify_ssl	Select one of the following: • True • False

Once configured to connect to your AWS CloudTrail, this connector can be used to perform the following actions:

Action	Description
Add Tags	Adds one or more tags to a trail, up to a limit of 50. Overwrites an existing tag's value when a new value is specified for an existing tag key. Tag key names must be unique for a trail; you cannot have two keys with the same name but different values.
Create Trail	Creates a trail that specifies the settings for delivery of log data to an Amazon S3 bucket.
Delete Trail	Deletes a trail. This operation must be called from the region in which the trail was created. DeleteTrail cannot be called on the shadow trails (replicated trails in other regions) of a trail that is enabled in all regions.
Get Trail Status	Returns a JSON-formatted list of information about the specified trail.
List Trails	Lists trails that are in the current account.
Lookup Events	Looks up management events or CloudTrail Insights events that are captured by CloudTrail. You can look up events that occurred in a region within the last 90 days. This action is configurable with *Data Ingestion*. You must enable the AWS CloudTrail Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Lookup Events (AWS CloudTrail Connector)* playbook will run according to the data ingestion schedule.

Action	Description
	When the playbook runs for the first time, the *AWS CloudTrail Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *AWS CloudTrail Log Parser* assignment. On this first run of the playbook, the connector will ingest events from the last seven days. In subsequent runs, it will ingest only new or updated events since the last run. The ingested logs can be viewed in *Log View > Logs > All*. The logs can be found using the following filter: `data_parsername="AWS CloudTrail Log Parser"`.
Start Logging	Starts the recording of Amazon Web Services API calls and log file delivery for a trail.
Stop Logging	Suspends the recording of Amazon Web Services API calls and log file delivery for the specified trail.
Update Trail	Updates trail settings that control what events you are logging, and how to handle log files.

AWS CloudWatch Logs connector

AWS CloudWatch Logs helps you monitor, store, and access your system, application, and custom log files. This connector facilitates automated operations related to the log group, log streams, and metrics. The connector's data ingestion option allows to ingest the CloudWatch logs into FortiAnalyzer. For more information, please refer to the Amazon CloudWatch Logs API Reference.

The AWS CloudWatch Logs connector is available as part of version 25.07004 content pack. It has further version updates in the following content pack:

- 25.08008
- 25.09003
- 25.10004
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events > Automation > Active Connectors*.

The following options are used to configure the AWS CloudWatch Logs connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
aws_access_key	Enter the access key.

Option	Description
aws_iam_role	Enter the IAM role.
aws_region	Enter the region.
aws_secret_access_key	Enter the secret access key.
config_type	Select one of the following: • IAM Role • Access Credentials
log_group_name	Enter the log group name.
log_stream_name	Enter the log stream name.
verify_ssl	Select one of the following: • True • False

Once configured to connect to your AWS CloudWatch Logs, this connector can be used to perform the following actions:

Action	Description
Create Log Group	Creates a log group based on the name you have specified. You can validate the log group creation at CloudWatch > Log Groups.
Create Log Stream	Creates a log stream based on the log group and the log stream name you have specified. You can validate the log stream creation at CloudWatch > Log Groups > Log Streams.
Delete Log Group	Deletes a log group, and it's associated archived log events, permanently based on the log group name you have specified. You can validate the log group's removal from CloudWatch > Log Groups.
Delete Log Stream	Deletes the log stream and it's associated archived log events based on the log group and the log stream name you have specified. Validate log stream removal at CloudWatch > Log Groups > Log Streams.
Get Log Events	Gets all the log events, or logs for the duration and the log stream you have specified. You can view the log event entries at CloudWatch > Log Groups > Log Stream > Log Event. This action is configurable with *Data Ingestion*. You must enable the AWS CloudWatch Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Get Log Events (AWS CloudWatch Logs Connector)* playbook will run according to the data ingestion schedule.

Action	Description
	When the playbook runs for the first time, the *AWS CloudWatch Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *AWS CloudWatch Log Parser* assignment. On this first run of the playbook, the connector will ingest events from the last seven days. In subsequent runs, it will ingest only new or updated events since the last run. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="AWS CloudWatch Log Parser"`.
Get Log Groups List	Gets a list of the log groups based on the log group name's prefix and the number of results to display on a page. You can list all the log groups or filter the results by log group name's prefix.
Get Log Insight Query Result	Gets results of a log insight query based on the query ID that you have specified.
Get Log Streams List	Gets a list of the log streams for a specified log group based on the log group name you and the list order you have specified. You can list all the log streams or filter the results log group name's prefix.
Revert Log Retention Policy	Reverts the retention of the specified log group based on the log group name you have specified. Log events do not expire if they belong to log groups without a retention policy.
Run Log Insight Query	Runs a query to get log insights using CloudWatch Logs Insights based on the comma-separated log group names, time range, and the query you have specified.
Stop Log Insight Query	Stops a CloudWatch Logs Insights query that is in progress based on the query ID you have specified.
Update Log Retention Policy	Sets a retention policy that retains log events based on the log group name and the number of days to retain.
Upload Log Event	Uploads log events to the log stream based on the log's group name and the stream name specified. You can upload multiple logs by specifying a sequence ID.

AWS Security Hub connector

AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards. The connector's data ingestion option allows to ingest the security findings into FortiAnalyzer. For more information, please refer to the AWS Security Hub API Reference.

The AWS Security Hub connector is available as part of version 25.06006 content pack. It has further version updates in the following content pack:

- 25.08008
- 25.09003
- 25.10004
- 26.01002
- 26.02002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the AWS Security Hub connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
AWS Access Key ID	Enter the access key ID.
AWS Instance IAM Role	Enter the IAM role.
AWS Region	Enter the region.
AWS Secret Access Key	Enter the secret access key.
Configuration Type	Select one of the following: • IAM Role • Access Credentials
Verify SSL	Select one of the following: • True • False

Once configured to connect to your AWS Security Hub, this connector can be used to perform the following actions:

Action	Description
Batch Update Findings	Update information about their investigation into a finding.
Disable Security Hub	Disables Security Hub in your account only in the current Region.
Enable Security Hub	Enables Security Hub for your account in the current Region or the Region you specify in the request.
Get Findings	Returns a list of findings that matches the specified criteria. This action is configurable with *Data Ingestion*. You must enable the AWS Security Hub Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Get Findings (AWS Security Hub Connector)* playbook will run according to the data ingestion schedule.

Action	Description
	When the playbook runs for the first time, the *AWS Security Hub Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *AWS Security Hub Log Parser* assignment. On this first run of the playbook, the connector will ingest logs from the last seven days. In subsequent runs, it will ingest only new or updated logs since the last run. The ingested logs can be viewed in *Log View > Logs > All*. The logs can be found using the following filter: `data_parsername="AWS Security Hub Log Parser"`.
Get Insights	Lists and describes insights for the specified insight ARNs.
Import Findings	Imports security findings generated from an integrated product into Security Hub. The maximum allowed size for a finding is 240 KB.
List Members	Lists details about all member accounts for the current Security Hub administrator account.

AWS SQS connector

Amazon Simple Queue Service (SQS) is a fully managed message queuing service. Connector actions allows you to scale and decouple microservices for distributed systems and serverless applications. For more information, please refer to the Amazon Simple Queue Service API Reference.

The AWS SQS connector is available as part of version 25.08008 content pack. It has a further version update in the following content pack:

- 25.09003
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events > Automation > Active Connectors*.

The following options are used to configure the AWS SQS connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
aws_access_key	Enter the access key.
aws_region	Enter the region.
aws_secret_access_key	Enter the secret access key.
verify_ssl	Select one of the following:

Option	Description
	• True • False

Once configured to connect to your AWS SQS, this connector can be used to perform the following actions:

Action	Description
Add Permission to Queue	Adds a permission to an existing queue for a principal that you have specified in your AWS account.
Add Tag to Queue	Adds a cost allocation tag to the Amazon SQS queue that you have specified.
Create Queue	Creates a new FIFO, or standard, message queue based on the inputs parameters you have specified, in your AWS account.
Delete Message	Deletes a message from the queue, based on the input parameters that you have specified from your AWS account.
Delete Queue	Deletes the queue that you have specified from your AWS account.
Get Dead-Letter Queues	Retrieves a list and details of queues from your AWS account that have the Redrive Policy queue attribute configured with a dead-letter queue.
Get List of Queues	Retrieves a list and details of all queues (or a list of queues based on the queue name prefix you have specified) associated with your AWS account.
Get Queue Attributes	Retrieves attributes for a queue that you have specified, from your AWS account.
Get Queue Tags	Retrieves a list all cost allocation tags added to the Amazon SQS queue that you have specified.
Get Queue URL	Retrieves the URL for an existing queue that you have specified, from your AWS account.
Purge Queue	Deletes all the messages from the queue that you have specified in your AWS account.
Receive Message	Retrieves one or more messages (up to 10 messages) from a specified queue in your AWS account.
Remove Permission	Revokes any permissions in the queue policy that matches the Label parameter that you have specified from your AWS account.
Remove Tag from Queue	Removes a cost allocation tag from the Amazon SQS queue that you have specified.
Send Message	Delivers a message to a queue that you have specified in your AWS account.
Update Queue	Updates a FIFO, or standard, message queue based on the inputs parameters you have specified, in your AWS account.

Azure Event Hub connector

Azure Event Hub Connector provides the option to ingest events across all partitions within a defined enqueued time window, using the Python SDK in synchronous batch mode. For more information, please refer to Azure Event Hubs client library for Python.

The Azure Event Hub connector is available as part of version 25.09003 content pack. It has further version updates in the following content pack:

- 25.10004
- 26.01002

This connector can be used in FortiAnalyzer 7.6.4 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Azure Event Hub connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
connection_str	Enter the connection string from your Azure portal.
consumer_group	Enter the consumer group for the event bub.
eventhub_name	Enter the event hub name.

Once configured to connect to your Azure Event Hub, this connector can be used to perform the following actions:

Action	Description
Ingest Events	Ingests events from the Azure Event Hub that were enqued within the specified timeframe. This action is configurable with *Data Ingestion*. You must enable the Azure Event Hub Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Ingest Events (Azure Event Hub Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Azure Event Hub Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *Azure Event Hub Log Parser* assignment. On this first run of the playbook, the connector will ingest events from the last seven days. In subsequent runs, it will ingest only new or updated events since the last run. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="Azure Event Hub Log Parser"`.

Azure Sentinel connector

Azure Sentinel is cloud-native SIEM for intelligent security analytics for your entire enterprise. This connector connects to Azure Sentinel using the Microsoft Graph API to investigate alerts, threat intelligence indicators, incidents, and secure score. For more information, please refer to Microsoft Sentinel API documentation.

The Azure Sentinel connector is available as part of version 25.10004 content pack. It has further version updates in the following content pack:

- 26.01002

This connector can be used in FortiAnalyzer 7.6.4 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Azure Sentinel connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
Client ID	Enter the Azure Sentinel client ID.
Client Secret	Enter the Azure Sentinel client secret.
Tenant ID	Enter the Azure Sentinel tenant ID.

Once configured to connect to your Azure Sentinel, this connector can be used to perform the following actions:

Action	Description
Create Threat Intelligence Indicator	Creates a threat intelligence indicator in Azure Sentinel using the Microsoft Graph Security API based on the threat type, indicator observables, and other input parameters you have specified.
Delete Threat Intelligence Indicator	Deletes a specific threat intelligence indicator from Azure Sentinel using the Microsoft Graph Security API based on the threat Intelligence Indicator ID you have specified.
Fetch Alert Query	Retrieves the query for a specific alert from Azure Sentinel based on the workspace ID and system alert ID that you have specified.
Get Alert	Retrieves a specific alert from Azure Sentinel using the Microsoft Graph Security API based on the Alert ID you have specified.
Get Alert Events	Retrieves all events associated with a specific alert from Azure Sentinel based on the workspace ID and search query that you have specified.
Get Alert List	Retrieves all alerts or alerts from Azure Sentinel based on the search query and other input parameters that you have specified. This action is configurable with *Data Ingestion*.

Action	Description
	You must enable the Azure Sentinel Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Get Alert List (Azure Sentinel Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Azure Sentinel Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *Azure Sentinel Log Parser* assignment. On this first run of the playbook, the connector will ingest logs from the last seven days. In subsequent runs, it will ingest only new or updated logs since the last run. The ingested logs can be viewed in *Log View > Logs > All*. The logs can be found using the following filter: `data_parsername="Azure Sentinel Log Parser"`.
Get All Secure Score Control Profiles	Retrieves all secure score control profiles from Azure Sentinel using the Microsoft Graph Security API.
Get All Secure Scores	Retrieves all secure scores associated with a specific Azure Tenant from Azure Sentinel using the Microsoft Graph Security API based on the Azure Tenant ID you have specified.
Get All Threat Intelligence Indicators	Retrieves all threat intelligence indicators from Azure Sentinel using the Microsoft Graph Security API.
Get Incident	Retrieves an incident associated with a specific alert from Azure Sentinel based on the incident ID, workspace name ID, and other input parameters you have specified.
Get Incident List	Retrieves all incidents from Azure Sentinel based on the workspace subscription ID, workspace name, and other input parameters that you have specified.
Get Threat Intelligence Indicator	Retrieves a specific threat intelligence indicator from Azure Sentinel using the Microsoft Graph Security API based on the threat Intelligence Indicator ID you have specified.
Update Alert	Updates a specific alert in Azure Sentinel using the Microsoft Graph Security API based on the alert ID, status, and other input parameters you have specified.
Update Incident	Updates an incident in Azure Sentinel based on the incident ID, workspace name ID, and other input parameters you have specified.
Update Threat Intelligence Indicator	Updates a specific threat intelligence indicator in Azure Sentinel using the Microsoft Graph Security API based on the threat intelligence indicator ID, and other input parameters you have specified.

Cisco Duo MFA connector

Cisco Duo generates multi-factor authentication (MFA) logs including access requests, verifications, and policy enforcement. For more information, please refer to the Duo Admin API Reference.

The Cisco Duo MFA connector is available as part of version 25.09003 content pack. It has further version updates in the following content pack:

- 25.10004
- 26.01002

This connector can be used in FortiAnalyzer 7.6.4 and later. It can be configured from *Incidents & Events > Automation > Active Connectors*.

The following options are used to configure the Cisco Duo MFA connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for your Cisco Duo MFA API.
Verify SSL	Enable to verify SSL.
integration_key	Enter the integration key from your Cisco Duo MFA.
secret_key	Enter the secret key from your Cisco Duo MFA.

Once configured to connect to your Cisco Duo MFA, this connector can be used to perform the following actions:

Action	Description
Ingest Authentication Logs	Ingest authentication log events. This action is configurable with *Data Ingestion*. You must enable the Cisco Duo MFA Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Ingest Authentication Logs (Cisco Duo MFA Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Cisco Duo MFA Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *Cisco Duo MFA Log Parser* assignment. On this first run of the playbook, the connector will ingest authentication logs from the last seven days. In subsequent runs, it will ingest only new or updated authentication logs since the last run. The ingested logs can be viewed in *Log View > Logs > All*. The logs can be found using the following filter: `data_parsername="Cisco Duo MFA Log Parser"`.

Cisco ISE connector

The Cisco ISE connector provides actions such as list all active sessions, quarantine IP/Mac address, un-quarantine IP/Mac address, and more. For more information, please refer to the Cisco ISE API Framework.

This connector relies on REST APIs introduced in Cisco ISE version 2.x or higher, which may be not available in earlier releases.

The Cisco ISE connector is available as part of version 25.06006 content pack. It has a further version update in the following content pack:

- 25.09003
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Cisco ISE connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Cisco ISE.
Port	Enter the Cisco ISE port.
User Name	Enter the Cisco ISE user name.
Password	Enter the Cisco ISE password.

Once configured to connect to your Cisco ISE, this connector can be used to perform the following actions:

Action	Description
Assign ANC Policy	Assigns a specific ANC policy to a MAC address or an IP address on Cisco ISE based on the policy or name and the MAC or IP address you have specified.
Create ANC Policy	Creates an ANC policy in Cisco ISE based on the ANC policy name and action you have specified.
Disable Internal User	Sets the status of an internal user to 'Disabled' in Cisco ISE based on the username you have specified.
Enable Internal User	Sets the status of an internal user to 'Enabled' in Cisco ISE based on the username you have specified.
End a Target MAC Address Session	Ends a session of the MAC address that you have specified on Cisco ISE.

Action	Description
Get All ANC Endpoints	Retrieves details for all Adaptive Network Control (ANC) endpoints from Cisco ISE.
Get All ANC Policies	Retrieves details for all ANC policies from Cisco ISE based on the policy ID or name and other input parameters you have specified.
Get All Endpoints	Retrieves details for all ERS endpoints on Cisco ISE.
Get ANC Endpoint	Retrieves details for a specific Adaptive Network Control (ANC) endpoint from Cisco ISE based on the ANC Endpoint ID and other input parameters you have specified.
Get ANC Policy	Retrieves details for a specific ANC policy from Cisco ISE based on the policy ID or name and other input parameters you have specified.
Get Endpoint	Retrieves details for a specific endpoint from Cisco ISE based on the endpoint ID or name and other input parameters you have specified.
Get Guest User Details	Retrieves details of a guest user from Cisco ISE based on the user ID you have specified.
Get Internal User Details	Retrieves details of an internal user fromCisco ISE based on the user ID you have specified.
List All Active Sessions	Retrieves a list of all active sessions from Cisco ISE.
List Guest Users	Retrieves all guest users or specific guest users from Cisco ISE based on your specified input parameters.
List Internal Users	Retrieves all internal users or specific internal users from Cisco ISE based on your specified input parameters.
MAC Address Logout	Logs off a session of the MAC address that you have specified on Cisco ISE.
Revoke ANC Policy	Revokes a specific ANC policy from a MAC address or an IP address on Cisco ISE based on the policy or name and the MAC or IP address you have specified.

FortiNDR Cloud connector

FortiNDR Cloud is a cloud-native network detection and response solution built for the rapid detection of threat activity, investigation of suspicious behavior, proactive hunting for potential risks, and directing a fast and effective response to active threats. This connector facilitates automated operation related to detection, entity, and sensors. For more information, please refer to the FortiNDR Cloud APIs in the FortiNDR Cloud User Guide.

The FortiNDR Cloud connector is available as part of version 26.04003 content pack. It has further version updates in the following content pack:

- 26.05003

This connector can be used in FortiAnalyzer 8.0.0 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the FortiNDR Cloud connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
API Key	Enter the API key for the FortiNDR Cloud instance.
Verify SSL	Enable to verify SSL.
Status	Enable or disable the connector.
Cloud Region	Select the cloud region to be used to access the FortiNDR Cloud APIs and perform the automated operations. You can choose either US Region or EU Region. For details, see the FortiNDR Cloud API Getting Started Documenation.
Account UUID	Specify the UUID of the account used to access FortiNDR Cloud and perform the automated operations. Note that it's required for actions like Get Devices with Detection, Get Entity Tracking, and so on.

Once configured to connect to your Cisco ISE, this connector can be used to perform the following actions:

Action	Description
Delete PCAP Task	Permanently removes a specific PCAP task and all its associated files from FortiNDR Cloud based on the task UUID that you have specified.
Get Detection Events	Retrieves a list of all detection events or specific detection events from FortiNDR Cloud based on the detection UUID and other input parameters you have specified.
Get Detection Rule Details	Retrieves information for a specific detection rule from FortiNDR Cloud based on the rule UUID and rule account UUID (optional) you have specified.
Get Detection Rule Events List	Retrieves a list of all events for a specific detection rule from FortiNDR Cloud based on the rule UUID and other input parameters you have specified.
Get Detection Rule Indicators	Retrieves a list of all detection rule indicators or specific detection rule indicators from FortiNDR Cloud based on the rule UUID and other input parameters you have specified.
Get Detection Rules List	Retrieves a list of all the detection rules or specific detection rules from FortiNDR Cloud based on the input parameters you have specified.
Get Detections List	Retrieves a list of all detections or specific detections from FortiNDR Cloud based on the input parameters you have specified. This action is configurable with *Data Ingestion*.

Action	Description
	You must enable the FortiNDR Cloud Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The Get Detections List playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the FortiNDR Cloud Log Parser is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the FortiNDR Cloud Log Parser assignment. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="FortiNDR Cloud Log Parser"`.
Get Devices with Detection	Retrieves a list of all devices with detection or specific devices with detection from FortiNDR Cloud based on the account UUID and other input parameters you have specified.
Get Entity Summary	Retrieves summary information about an IP address or domain from FortiNDR Cloud based on the IP address or Domain you have specified.
Get Entity Tracking	Retrieves information about an IP address, MAC address, or Host name from FortiNDR Cloud based on the entity type and value and other input parameters you have specified.
Get Passive DNS Details	Retrieves passive DNS information about an IP address or domain from FortiNDR Cloud based on the IP address or Domain and other input parameters you have specified.
Get PCAP Tasks	Retrieves a list of all the PCAP tasks or specific PCAP tasks from FortiNDR Cloud based on the input parameters you have specified.
Get Sensors List	Retrieves a list of all sensors or specific sensors from FortiNDR Cloud based on the input parameters that you have specified.
Get Telemetry Bandwidth	Retrieves details of telemetry bandwidth from FortiNDR Cloud based on the input parameters you have specified.
Get Telemetry Events	Retrieves details for all telemetry events or specific telemetry events from FortiNDR Cloud based on the input parameters you have specified.
Get Telemetry Packetstats	Retrieves details for telemetry packetstats from FortiNDR Cloud based on the input parameters you have specified.
Resolve Detection	Resolves a specific detection on FortiNDR Cloud based on the detection UUID, resolution, and comment (optional) you have specified.
Terminate PCAP Task	Stops a specific, currently running, PCAP task on FortiNDR Cloud based on the task UUID that you have specified.

Fresh Service Desk MSP connector

Fresh Service Desk MSP is a cloud-based service desk and IT service management (ITSM) platform designed to streamline service management for businesses. It offers a range of features including incident management, problem management, change management, asset management, and more. The connector for Freshservice enables automated actions such as creating, updating, deleting, and closing tickets, enhancing the efficiency of service delivery for managed service providers. For more information, please refer to the Freshservice API reference.

The Fresh Service Desk MSP connector is available as part of version 25.05005 content pack. It has a further version update in the following content pack:

- 25.09003
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Fresh Service Desk MSP connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Fresh Service Desk MSP.
User Name	The Fresh Service Desk MSP user name.
API Key	The API key for the Fresh Service Desk MSP.

Once configured to connect to your Fresh Service Desk MSP, this connector can be used to perform the following actions:

Action	Description
Create Ticket	Creates a ticket in Fresh Service Desk MSP based on the requester, subject, and other input parameters you have specified.
Delete Ticket	Delete of specific tickets from Fresh Service Desk MSP on the input parameters you have specified.
Filter Tickets By Query	Retrieves list of tickets matching the specified query.
Get Ticket Details	Retrieves details of specific tickets from Fresh Service Desk MSP on the input parameters you have specified.
Update Ticket	Update a ticket in Fresh Service Desk MSP based on the ticket id and other input parameters you have specified.

Google Cloud PubSub connector

Google Cloud Pub/Sub delivers messaging service logs for publishing, subscription, and message delivery events. For more information, please refer to the Cloud Pub/Sub API Reference.

The Google Cloud PubSub connector is available as part of version 25.09003 content pack. It has further version updates in the following content pack:

- 25.10004
- 26.01002

This connector can be used in FortiAnalyzer 7.6.4 and later. It can be configured from *Incidents & Events > Automation > Active Connectors*.

The following options are used to configure the Google Cloud PubSub connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for your Google Cloud Pub/Sub.
Verify SSL	Enable to verify SSL.
client_id	Enter the client ID.
client_secret	Enter the client secret.
code	Enter the client code.
redirect_url	Enter the redirect URL.
subscription_name	Enter the subscription name.

Once configured to connect to your Google Cloud PubSub, this connector can be used to perform the following actions:

Action	Description
Acknowledge Messages from Subscriptions	Acknowledges messages from a specific subscription in Google Pub/Sub based on the subscription name and acknowledge IDs you have specified.
Create Snapshots	Creates a snapshot on your configured Google Cloud Pub/Sub server based on the project ID, snapshot name, subscription name, and other input parameters you have specified.
Create Subscription	Creates a subscription on your configured Google Cloud Pub/Sub server based on the project ID, subscription name, topic name, and other input parameters you have specified.
Create Topic	Creates a topic on your configured Google Cloud Pub/Sub server based on the project ID, topic name, and other input parameters you have specified.

Action	Description
Delete Snapshots	Deletes an existing snapshot on your configured Google Cloud Pub/Sub server based on the snapshot name you have specified.
Delete Subscription	Deletes an existing subscription on your configured Google Cloud Pub/Sub server based on the subscription name you have specified.
Delete Topic	Deletes a specific topic from your configured Google Cloud Pub/Sub server based on the topic name you have specified.
Get Subscription Details	Retrieves information for a specific subscription from Google Pub/Sub based on the subscription name you have specified.
Get Topic Details	Retrieves information for a specific topic from Google Pub/Sub based on the topic name you have specified.
List All Snapshots	Retrieves a list of snapshots associated with a specific project from Google Pub/Sub based on the project ID and other input parameters you have specified.
List All Subscriptions	Retrieves a list of subscriptions associated with a specific project from Google Pub/Sub based on the project ID and other input parameters you have specified.
List All Topic Snapshots	Retrieves a list of snapshots associated with a topic from Google Pub/Sub based on the topic and other input parameters you have specified.
List All Topic Subscriptions	Retrieves a list of subscriptions associated with a specific topic from Google Pub/Sub based on the topic name and other input parameters you have specified.
List All Topics	Retrieves a list of topics associated with a specific project from Google Pub/Sub based on the project ID and other input parameters you have specified.
Publish Messages to Topic	Adds one or more messages to a specific topic in Google Pub/Sub based on the topic name and messages you have specified.
Pull Messages from Subscriptions	Retrieves a list of pull messages associated with a specific subscription from Google Pub/Sub based on the subscription name and size parameter you have specified. This action is configurable with *Data Ingestion*. You must enable the Google Cloud PubSub Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Pull Messages from Subscriptions (Google Cloud PubSub Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Google Cloud PubSub Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *Google Cloud PubSub Log Parser* assignment.

Action	Description
	On this first run of the playbook, the connector will ingest messages from the last seven days. In subsequent runs, it will ingest only new or updated messages since the last run. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="Google Cloud PubSub Log Parser"`.
Seeks Subscriptions	Seeks an existing subscription in Google Pub/Sub based on the subscription name and other input parameters you have specified. Note: Both the subscription and the snapshot must be on the same topic.
Update Snapshots	Updates a snapshot on your configured Google Cloud Pub/Sub server based on the snapshot name, subscription name, topic name, and other input parameters you have specified.
Update Subscription	Updates a subscription on your configured Google Cloud Pub/Sub server based on the project ID, subscription name, topic name, and other input parameters you have specified.
Update Topic	Updates a specific topic on your configured Google Cloud Pub/Sub server based on the topic name, fields that you want to update, and other input parameters you have specified.

Grafana connector

Grafana Alerting Service provides a unified, powerful system for monitoring and notifying users, allowing them to fetch alert data, including the status and details of active or past alerts. For more information, please refer to the Grafana HTTP API reference.

The Grafana connector is available as part of version 26.01002 content pack.

This connector can be used in FortiAnalyzer 7.6.5 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Grafana connector:

Option	Description
IP/FQDN	Enter the IP or fully qualified domain name for your Grafana instance.
API Key	Enter the API key for the Grafana instance.
Verify SSL	Enable to verify SSL.
Port Number	Enter the port number.

Once configured to connect to your Grafana service, this connector can be used to perform the following actions:

Action	Description
Execute an API Request	Sends an API request to any API endpoint based on specified HTTP method, endpoint, and other input parameters that you have specified, enabling flexible API interactions tailored to user needs.
Get Alerts	Retrieves a list of Grafana alerts and the current status of active alerts across all alerting rules from the Grafana instance.
Get Data Sources	Retrieves a list of configured data sources from the Grafana instance.
Run Data Source Query	Executes one or more queries on specified data sources based on provided input parameters.

Jira connector

The Jira Service Desk Connector can be used creating, updating, and deleting issues. For more information, please refer to the Jira Service Management REST API.

The Jira Connector is introduced in the version 25.03004 content pack. It has further version updates in the following content pack:

- 25.04006
- 25.09003
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Jira Connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Jira Service Desk.
User Name	Enter the Jira Service Desk user name.
api_key	Enter the API key for the Jira Service Desk.

Once configured to connect to your Jira Service Desk, this connector can be used to perform the following actions:

Action	Description
Add Comment	Adds a comment to an existing Jira ticket on your configured Jira server based on the ticket ID and comment you have specified.

Action	Description
Add Remote Link	Adds a remote link of an issue to an existing ticket in Jira based on the ticket ID, URL, and title you have specified.
Assign Issue to User	Assigns an issue to a user based on the account and ticket ID that you have specified.
Create Ticket	Creates a Jira ticket on your configured Jira server based on the project key, ticket summary, type, and description, and other input parameters you have specified.
Delete Ticket	Deletes a ticket from your configured Jira server based on the ticket ID and other input parameters you have specified.
Get Comments	Retrieves a list of comments associated with an existing Jira ticket on your configured Jira server based on the ticket ID and other input parameters you have specified.
Get Ticket Details	Retrieves details for a particular Jira ticket from the Jira server based on the ticket ID you have specified.
Get User Details	Retrieves details for a particular Jira user from the Jira server based on the account ID you have specified.
List Projects	Retrieves a list and details of all projects from your configured Jira server.
List Tickets	Retrieves a list and details of tickets associated with a project from your configured Jira server, based on the project key and other input parameters you have specified.
Search Users	Returns a list of all users, including active users, inactive users and previously deleted users that have an Atlassian account.
Set Ticket Status	Updates the status of an existing Jira ticket on your configured Jira server based on the ticket ID and status you have specified.
Update Ticket	Updates an existing Jira ticket on your configured Jira server based on the project key, ticket ID and other input parameters you have specified.
Validate JQL query	Parses and validates JQL query syntax and returns errors when found.

ManageEngine ServiceDesk Plus - MSP connector

ManageEngine ServiceDesk Plus MSP is a web based, full-fledged ITSM suite designed specifically for managed service providers. This all-in-one ITSM solution delivers comprehensive help desk, service desk, account management, asset management, remote controls and advanced reporting in a multi-tenant architecture with robust data segregation. For more information, please refer to the ServiceDesk Plus REST API - User Guide.

The ManageEngine ServiceDesk Plus - MSP connector is available as part of version 25.04006 content pack. It has a further version update in the following content pack:

- 25.09003
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the ManageEngine ServiceDesk Plus - MSP connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the ManageEngine ServiceDesk Plus - MSP.
API Key	The API key for the ManageEngine ServiceDesk Plus - MSP.

Once configured to connect to your ManageEngine ServiceDesk Plus - MSP, this connector can be used to perform the following actions:

Action	Description
Add Note	Adds a note to an existing ticket in ServiceDesk Plus MSP based on the ticket request ID, description, and other input parameters you have specified.
Add Resolution	Adds a resolution to an existing ticket in ServiceDesk Plus MSP based on the ticket request ID and resolution you have specified.
Close Ticket	Closes a ticket in ServiceDesk Plus MSP based on the ticket request ID and other input parameters you have specified.
Create Ticket	Creates a ticket in ServiceDesk Plus MSP based on the requester, subject, and other input parameters you have specified.
Delete Ticket	Deletes a ticket (moves it to Trash) from ServiceDesk Plus MSP based on the ticket request ID you have specified.
Delete Ticket From Trash	Permanently deletes a ticket from the Trash in ServiceDesk Plus MSP based on the Ticket Request ID you have specified.
Get All Sites	Retrieves information of all site details Service Desk Plus MSP.
Get All Tickets	Retrieves details of all tickets or specific tickets from ServiceDesk Plus MSP based on the input parameters you have specified.
Get All Users	Retrieves details of all users or specific user from ServiceDesk Plus MSP based on the input parameters you have specified.
Get Ticket Details	Retrieves details of a specific ticket from ServiceDesk Plus MSP based on the ticket request ID you have specified.
Update Ticket	Updates an existing ticket in ServiceDesk Plus MSP based on the ticket request ID and other input parameters you have specified.

Microsoft 365 Defender connector

The Microsoft 365 Defender connector facilitates the automation of operations related to files, machines, IP, domain, actor, etc., and supports the ingestion of Microsoft 365 Defender incidents into FortiAnalyzer. For more information, please refer to the Supported Microsoft Defender XDR APIs.

The Microsoft 365 Defender connector is available as part of version 25.05005 content pack. It has further version updates in the following content pack:

- 25.08008
- 25.09003
- 25.10004
- 26.01002
- 26.02002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events > Automation > Active Connectors*.

The following options are used to configure the Microsoft 365 Defender connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Microsoft 365 Defender.
Authentication Type	Select one of the following: • *Application - Without a User* • *Delegated - On behalf of User*
Client ID	Enter the client ID for the Microsoft 365 Defender.
Client Secret	Enter the client secret for the Microsoft 365 Defender.
Code	Enter the code. This field is only required when the *auth_type = Delegated - On behalf of User*.
Redirect URL	Enter the redirect URL. This field is only required when the *auth_type = Delegated - On behalf of User*.
Tenant ID	Enter the tenant ID for the Microsoft 365 Defender.

Once configured to connect to your Microsoft 365 Defender, this connector can be used to perform the following actions:

Action	Description
Advanced Hunting	Retrieves data from the past 30 days based on the query that you have specified.
Get Incident Details	Retrieves the details of a specific incident based on the incident ID that you have specified.
Get Incidents List	Retrieves a list of flagged network incidents with their status, allowing users to filter by time range, owner, and other details to support informed cybersecurity response. This action is configurable with *Data Ingestion*. You must enable the Microsoft 365 Defender Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Get Incidents List (Microsoft 365 Defender Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Microsoft 365 Defender Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *Microsoft 365 Defender Log Parser* assignment. On this first run of the playbook, the connector will ingest incidents from the last seven days. In subsequent runs, it will ingest only new or updated incidents since the last run. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="Microsoft 365 Defender Log Parser"`.
Update Incident	Updates the owner, status, comments, and other details of existing incidents based on the incident ID that you have specified.

Microsoft Graph API connector

The Microsoft Graph API connector can be used to access a wide range of data and services from Microsoft 365 and Azure Active Directory (Azure AD), with the option to ingest Microsoft Entra ID (previously known as Azure AD) logs to FortiAnalyzer. It provides a single endpoint and a consistent set of RESTful web APIs, to integrate with Microsoft's cloud services and applications. For more information, please refer to Microsoft Graph REST API.

The Microsoft Graph API connector is available as part of version 25.03004 content pack. It has further version updates in the following content pack:

- 25.08008
- 25.09003
- 25.10004
- 26.01002
- 26.02002

This connector can be used in FortiAnalyzer 7.6.2 and later. It can be configured from *Incidents & Events > Automation > Active Connectors*.

The following options are used to configure the Microsoft Graph API connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Microsoft Graph API.
Verify SSL	Enable to verify SSL.
Authentication Type	Select one of the following: • *Application - Without a User* • *Delegated - On behalf of User*
Client ID	Enter the client ID for the Microsoft Graph API.
Client Secret	Enter the client secret for the Microsoft Graph API.
Authorization Code	Enter the code. This field is only required when the *auth_type = Delegated - On behalf of User*.
Redirect URL	Enter the redirect URL. This field is only required when the *auth_type = Delegated - On behalf of User*.
Tenant ID	Enter the tenant ID for the Microsoft Graph API.

Once configured to connect to your Microsoft Graph API, this connector can be used to perform the following actions:

Action	Description
Block New IP Ranges	Blocks IPv4 and IPv6 address ranges in specified NamedLocation in Azure.
Create IP Named Location	Creates a new IP named location in Azure based on specified input parameter.
Delete Message	Deletes a specific message from the specific user's mailbox in Azure based on the user ID and message ID you have specified.
Delete Message Bulk	Deletes messages from multiple users mailboxes in Azure based on the comma-separated list of users you have specified.
Get All Named Locations	Retrieves a list of named location from Azure based on display name, sort order, and other input parameters that you have specified.
Get All Security Alerts	Retrieves a list of alerts from Microsoft Graph API based on the input parameters you have specified.
Get Groups	Retrieves a list of groups from Microsoft Graph API.

Action	Description
Get Risky User Details	Retrieve details for a specific risky user from Microsoft Graph API based on the user ID you have specified.
Get Risky Users List	Retrieves a list of all risky users from Microsoft Graph API.
Get Security Alert	Retrieves details of a specific alert from Microsoft Graph API based on the alert ID you have specified.
Get Users Within A Group	Retrieves a list of users within a specific group from Microsoft Graph API based on the group ID you have specified.
Ingest Microsoft Entra ID Logs	Ingest Microsoft Entra ID (previously known as Azure AD) Logs. This action is configurable with *Data Ingestion*. To use this action, you must enable the *Microsoft Entra ID Log Parser* and configure a data ingestion schedule for the connector action. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Ingest Microsoft Entra ID Logs (Microsoft Graph API Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Microsoft Entra ID Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the log parser assignment. On this first run of the playbook, the connector will ingest logs from the last seven days. In subsequent runs, it will ingest only new or updated logs since the last run. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="Microsoft Entra ID Log Parser"`.
Revoke User Session	Invalidates all the refresh tokens issued to applications for a user.
Search Message in Users Mailbox	Searches for messages in a user's mailbox within an organization based on the 'Subject' and user list you have specified.
Unblock IP Ranges	Unblocks IPv4 and IPv6 address ranges in specified NamedLocation in Azure.
Update Security Alert	Updates a specific alert using Microsoft Graph API based on the alert ID, vendor name, provider name, and other input parameters you have specified.

Microsoft Management Activity API connector

The Microsoft Management Activity API connector contains connector operator and playbook schemas needed to ingest Office 365 and Azure AD activity logs from Microsoft Management Activity API to FortiAnalyzer. For more information, please refer to Office 365 Management APIs.

The Microsoft Management Activity API connector is available as part of version 25.01009 content pack. It has further version updates in the following content packs:

- 25.02004
- 25.07004
- 25.08008
- 25.09003
- 26.01002
- 26.02002

This connector can be used in FortiAnalyzer 7.6.2 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Microsoft Management Activity API connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Microsoft Management Activity API.
Verify SSL	Enable to verify SSL.
Authentication Type	Select one of the following: • *Application - Without a User* • *Delegated - On behalf of User*
Client ID	Enter the client ID for the Microsoft Management Activity API.
Client Secret	Enter the client secret for the Microsoft Management Activity API.
Authorization Code	Enter the authorization code. This field is only required when the *auth_type = Delegated - On behalf of User*.
Redirect URL	Enter the redirect URL. This field is only required when the *auth_type = Delegated - On behalf of User*.
Tenant ID	Enter the tenant ID for the Microsoft Management Activity API.

Once configured to connect to your Microsoft Management Activity API, this connector can be used to perform the following actions:

Action	Description
Ingest Microsoft Management Activity API Logs	Ingest Office 365 and Azure AD activity logs from the Microsoft Management Activity API. This action is configurable with *Data Ingestion*. To use this action, you must enable the *Office 365 Management Activity Log Parser* and configure a data ingestion schedule for the connector action.

Action	Description
	Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The *Ingest Microsoft Management Activity API Logs (Microsoft Management Activity API Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Office 365 Management Activity Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the log parser assignment. On this first run of the playbook, all logs from the last 24 hours will be ingested. In subsequent runs of this action, only new logs since the last fetch will be ingested and added to FortiAnalyzer. The ingested logs can be viewed in *Log View > Logs > All*. The logs can be found using the following filter: `data_parsername="Office 365 Management Activity Log Parser"`.
MS Management Activity Start Subscription	Starts a subscription in Microsoft.
MS Management Activity Stop Subscription	Stops a subscription in Microsoft.
MS Management Activity List Subscription	Retrieves a current list of subscriptions in Microsoft.
MS Management Activity List Content	Retrieves content from Microsoft.

Nessus connector

Nessus Connector integrates with Tenable Nessus (Tenable.sc) to automatically ingest vulnerability scan results from all scanners. For more information, please refer to the Tenable API Explorer.

The Nessus connector is available as part of version 25.08008 content pack. It has a further version update in the following content pack:

- 25.09003
- 25.10004
- 26.01002

This connector can be used in FortiAnalyzer 7.6.4 and later. It can be configured from *Incidents & Events > Automation > Active Connectors*.

The following options are used to configure the Nessus connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Tenable Nessus (Tenable.sc).
User Name	Enter the user name.
Password	Enter the password.
Verify SSL	Enable to verify SSL.
access_key	Enter the access key.
secret_key	Enter the secret key.

Once configured to connect to your Tenable Nessus, this connector can be used to perform the following actions:

Action	Description
Get List of Scans	Retrieves a list of scans
Ingest Vulnerability Scan Results	Connects to the Nessus API to fetch scan metadata and detailed findings, filtering by creation or modification time to capture only new or updated scans. This action is configurable with *Data Ingestion*. You must enable the Nessus Log Parser to ingest logs using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm logs are ingested. The *Ingest Vulnerability Scan Results (Nessus Connector)* playbook will run according to the data ingestion schedule. When the playbook runs for the first time, the *Nessus Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *Nessus Log Parser* assignment. On this first run of the playbook, the connector will ingest vulnerability scan results from the last 30 days. In subsequent runs, it will ingest only new or updated results since the last run. The ingested logs can be viewed in *Log View > Logs > All*. The logs can be found using the following filter: `data_parsername="Nessus Log Parser"`.

ServiceNow Integration connector

ServiceNow generates incident, change, and service request logs, including ticket details, state transitions, priorities, and assignments. The ServiceNow Integration connector provides functionality to create, read,

update and delete records of Table and Catalog type. For more information, please refer to the ServiceNow REST API Reference.

The ServiceNow Integration connector is available as part of version 25.08008 content pack. It has a further version update in the following content pack:

- 25.09003
- 25.10004
- 26.01002

This connector can be used in FortiAnalyzer 7.6.4 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the ServiceNow Integration connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the ServiceNow Integration.
User Name	Enter the user name.
Password	Enter the password.
Verify SSL	Enable to verify SSL.

Once configured to connect to your ServiceNow, this connector can be used to perform the following actions:

Action	Description
Add Item to Cart	Adds an item to the cart and submits the order on ServiceNow.
Advanced Search	Executes a generalized query on the ServiceNow table that you have specified to search for a record in ServiceNow.
Create Incident	Adds a new incident record in ServiceNow based on the input parameters you have specified.
Create Table Record	Adds a new record in the ServiceNow table that you have specified.
Delete Cart Item	Deletes an item from a cart in ServiceNow based on the Cart Item ID you have specified.
Fetch Incidents	Fetches incidents from the ServiceNow incident table with a query. This action is configurable with *Data Ingestion*. You must enable the ServiceNow Log Parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm logs are ingested. The *Fetch Incidents (ServiceNow Integration Connector)* playbook will run according to the data ingestion schedule.

Action	Description
	When the playbook runs for the first time, the *ServiceNow Log Parser* is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the *ServiceNow Log Parser* assignment. On this first run of the playbook, the connector will ingest incidents from the last seven days. In subsequent runs, it will ingest only new or updated incidents since the last run. The ingested logs can be viewed in *Log View > Logs > All*. The logs can be found using the following filter: `data_parsername="ServiceNow Log Parser"`.
Get Assignment Groups	Retrieves a list and details of all existing assignments groups from ServiceNow.
Get Cart	Retrieves a default list of all existing cart contents, cart details, and price from ServiceNow.
Get Catalog Categories	Retrieves a list and details of all existing categories or the list and details of categories for a specified catalog from ServiceNow based on the Sys ID of the catalog you have specified.
Get Catalogs	Retrieves a list and details of catalogs to which the user has access from ServiceNow. You can optionally specify the Sys ID of the catalog to retrieve details only for a specific catalog.
Get Items	Retrieves a list of all existing catalogs and a list and details of all items that are contained in each catalog from ServiceNow. You can optionally specify the Sys ID of the item to retrieve details only for a specific item.
Get Users	Retrieves a list of users and their details from ServiceNow based on the response fields you have specified.
Search Table Record	Searches for a record in ServiceNow based on the table name, column name and value, and other input parameters you have specified.
Update Cart Item	Updates an item in a cart in ServiceNow based on the Cart Item ID and other input parameters you have specified.
Update ServiceNow Incident	Updates an incident ServiceNow table based on the Sys ID of the incident and other input parameters you have specified.
Update ServiceNow Table Record	Updates a record in the ServiceNow table based on the Sys ID of the table record and other input parameters you have specified.

Splunk

Splunk is a SIEM software that allows searching, monitoring, and analyzing machine-generated big data, using a web-style interface. For more information, please refer to the Splunk Enterprise REST API Reference.

The Splunk connector is available as part of version 26.03005 content pack.

This connector can be used in FortiAnalyzer 7.6.6 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Splunk connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for your Splunk application.
Port	Enter the port for connection with Splunk.
User Name	The Splunk user name.
Password	Enter the password for the Splunk user.
Verify SSL	Enable to verify SSL.
Application Namespace	Enter your Splunk application namespace.
Search Query	Enter the search query.
Protocol	Select https or http.

Once configured to connect to your Splunk application, this connector can be used to perform the following actions:

Action	Description
Add New Collection to Splunk App	Adds a new KVStore collection to a specified Splunk App, based on the application name, collection name, and other input parameters you have specified.
Add Record to a Collection	Adds a record to an existing KVStore collection within the specified Splunk App, based on the application name, collection name, record key and value, and other input parameters you have specified.
Bulk Add Record to a Collection	Adds one or more records to an existing KVStore collection within the specified Splunk App, based on the application name, collection name, record key value, and other input parameters you have specified.
Delete Record From a Collection	Removes a record from an existing KVStore collection within the specified Splunk App, based on the application name, collection name, record ID, and other input parameters you have specified.
Fetch Events	Fetches events from the Splunk server. This action is configurable with *Data Ingestion*. You must enable the Splunk log parser to ingest incidents using the connector. Once the log parser is enabled and the connector is configured with a data ingestion schedule, you can check the *Playbook Monitor* to confirm incidents are ingested. The Splunk Fetch Events playbook will run according to the data ingestion schedule.

Action	Description
	When the playbook runs for the first time, the Splunk log parser is automatically assigned to a device for data ingestion in *Assigned Parsers*. If this device already exists from a previously configured connector with data ingestion support, the same device will be used. If not, a new device will be automatically created for the Splunk log parser assignment. The ingested logs can be viewed in *Log View* > *Logs* > *All*. The logs can be found using the following filter: `data_parsername="Splunk Log Parser"`.
Fetch Records from Collection	Retrieves a list of all records of a specified collection within the specified Splunk App, based on the application name, collection name, and other input parameters you have specified.
Get All Collections from Splunk App	Retrieves a list containing all KVStore collections stored in the context of a specified Splunk App from Splunk, based on the application name and other input parameters you have specified.
Get Details for a Search	Retrieves the details for a Splunk search.
Get Details Of Triggered Alert	Retrieves information of an alert triggered on Splunk based on the name of the alert you have specified.
Get Events for a Search	Retrieves the event details for a Splunk search.
Get List Of Triggered Alerts	Retrieves a list of alerts that are triggered on Splunk based on the parameters you have specified.
Get Results for a Search	Retrieves the results for a Splunk search.
Get Splunk Action	Retrieves details of the available Splunk alert actions or adaptive response actions.
Invoke Search	Invokes a search on the Splunk server.
Run Splunk Action	Runs an alert action or an adaptive response action on a search result or a notable.

Zendesk connector

The Zendesk connector provides an automated way to create, read, update, mark spam, restore and delete tickets in Zendesk. For more information, please refer to the Zendesk API Reference.

The Zendesk connector is available as part of version 25.04006 content pack. It has a further version update in the following content pack:

- 25.09003
- 26.01002

This connector can be used in FortiAnalyzer 7.6.3 and later. It can be configured from *Incidents & Events* > *Automation* > *Active Connectors*.

The following options are used to configure the Zendesk connector:

Option	Description
Name	Enter a name for the connector or use the default.
Description	Enter a description for the connector or use the default.
IP/FQDN	Enter the IP or fully qualified domain name for the Zendesk.
User Name	The Zendesk user name.
API Key	The API key for the Zendesk.

Once configured to connect to your Zendesk, this connector can be used to perform the following actions:

Action	Description
Create Ticket	Create a new ticket in Zendesk with specified ticket properties.
Delete Bulk Of Tickets	Delete multiple tickets from a List of Deleted Tickets action. Accepts a comma-separated list of ticket ID's up to 100.
Delete Bulk Of Tickets Permanently	Permanently deletes up to 100 soft-deleted tickets.This action accepts a comma-separated list of up to 100 ticket ID's. If one ticket fails to be deleted, the action still attempts to delete the others.
Delete Ticket	Delete ticket using a ticket ID. You can delete 400 tickets every 1 minute using this action.
Delete Ticket Permanently	Delete ticket permanently from a List of Deleted Tickets action. If the job succeeds, the ticket is permanently deleted. This action can't be undone.
Get Deleted Ticket List	Returns a maximum of 100 deleted tickets per page.The results includes all deleted (and not yet archived) tickets that have not yet been scrubbed in the past 30 days.
Get Ticket Details	Get the details of specified ticket ID.
Get Ticket Related Details	Get related information of a given ticket ID.
Get Tickt List	To get list of all tickets from Zendesk. Returns maximum of 100 tickets per page.
Mark Ticket as Spam	Mark specified ticket as spam in Zendesk.
Restore Ticket	Restore a previously deleted ticket from List of Deleted Tickets action.
Update Ticket	Update an existing ticket with specified input parameters.

ZTNA Brute Force Login Investigation playbook

Playbook to investigate the alert source IP. If the source IP is malicious, the playbook will automatically raise an incident. VirusTotal connector configuration is required.

This playbook was introduced in content pack version 26.01002.

Requirements:

- The VirusTotal connector is configured
- The predefined ZTNA Brute Force Login handler is enabled
- FortiAnalyzer is 7.6.4 or later

The ZTNA Brute Force Login Investigation playbook is triggered when events are generated by the predefined ZTNA Brute Force Login handler.

This playbook is enabled by default and uses actions from the following connectors:

- Local Connector (FortiAnalyzer)
- VirusTotal Connector

www.fortinet.com