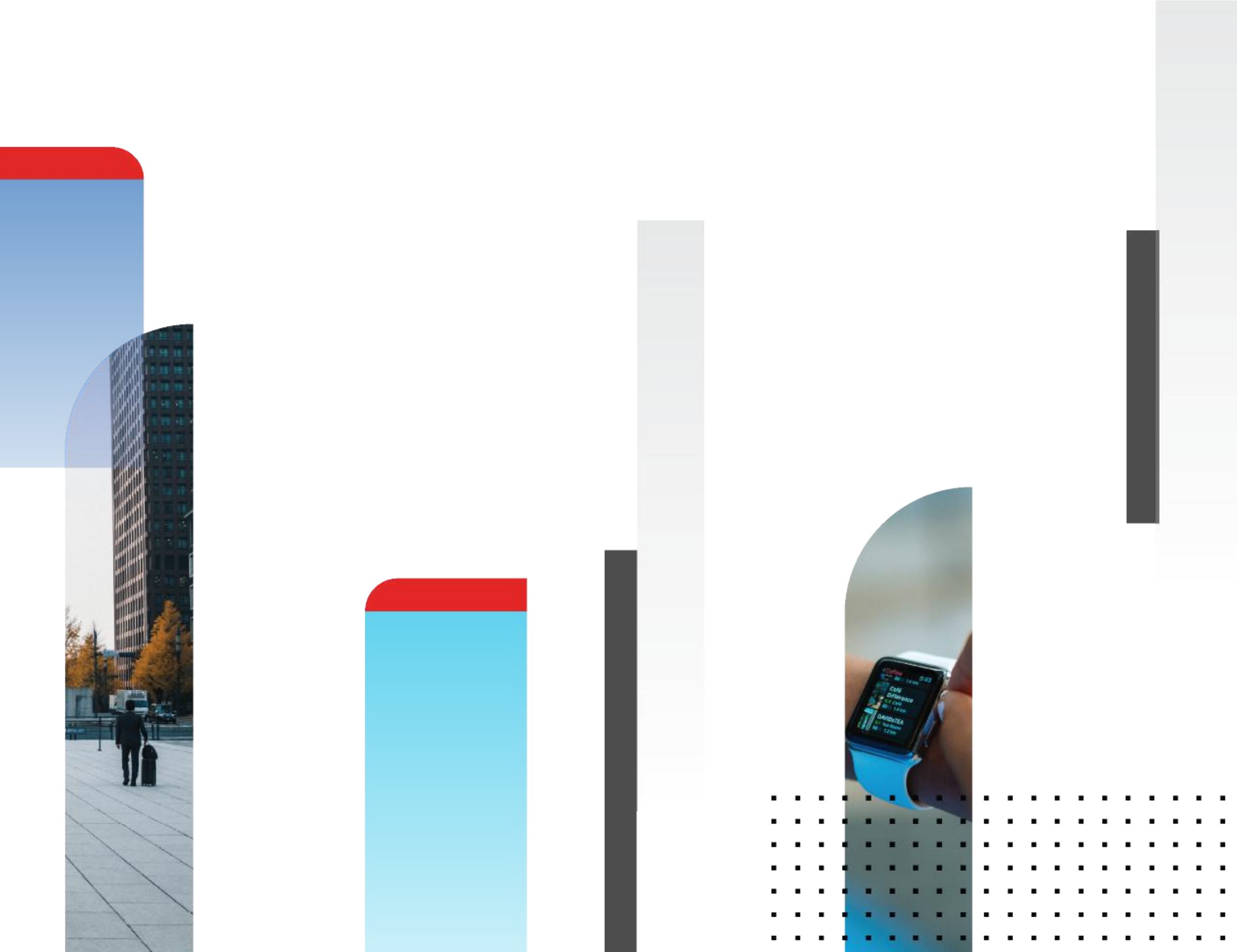
External Systems Configuration Guide

FortiSIEM 6.3.2



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

01/06/2022
FortiSIEM 6.3.2 External Systems Configuration Guide

Change Log

Date	Change Description
2018-05-23	Initial version of the guide.
2018-07-24	Revision 2 with a new section under Windows Server Configuration - Configuring Log Monitoring for Non-Administrative User.
2018-08-07	Revision 3 with updated section: Fortinet FortiGate Firewall
2018-09-12	Revision 4 with updated section: Microsoft Azure Audit
2018-09-26	Revision 5 with updated section: WatchGuard Firebox Firewall
2018-11-28	Revision 6 with updated section: Fortinet FortiGate Firewall > Configuring SSH on FortiSIEM to communicate with FortiGate
2019-01-29	Revision 7: updated section: Cisco FireSIGHT
2019-03-15	Revision 8: new section: Threat Intelligence
2019-03-28	Revision 9: updates the guide to reflect the new menu hierarchy in the FortiSIEM tool.
2019-04-24	Revision 10: added Carbon Black Security Platform under End Point Security Software.
2019-07-24	Revision 11: updated integration instructions for Microsoft Office 365 Audit.
2019-10-22	Revision 12: added Clavister Firewall and FortiADC devices. Added Active Directory User Discovery section to Microsoft Active Directory device. Corrections to SQL Server DDL Event Creation Script and SQL Server Database Level Event Creation Script.
2019-11-22	Revision 13: added Zeek (Bro) installation instructions for Security Onion, Cyberoam FortiADC, Epic SecuritySIEM, FortiEDR, FortiNAC, FortiDeceptor, Microsoft Network Policy Server, TrendMicro Deep Discovery. Changed the name of Cisco FireAMP to Cisco AMP Cloud V0. Changed the name of Cisco AMP to Cisco AMP Cloud V1.
2020-01-03	Revision 14: added CradlePoint.
2020-04-15	Revision 15: added Alert Logic Iris API, AWS Kinesis, AWS Security Hub, Cisco Amp, GitLab Cli, Azure Event Hub, Azure Compute, McAfee ePolicy Orchestrator, LastLine, Imperva Securesphere Web App Firewall, Imperva Securesphere DB Security Gateway, Imperva Securesphere DB Monitoring Gateway, Green League WVSS, FortiInsight, Damballa Failsafe, AWS EC2, Cisco Fireamp, Novell Netware, Green League RSAS, Checkpoint SmartCenter, FortiTester, Cisco Viptela, MobileIron, Duo, Indegy Industrial Cybersecurity Suite, Netwrix, Darktrace DCIP, Hirschmann SCADA Firewalls and Switches.
2020-07-22	Revision 16: Edits to Cisco AMP Cloud V0 and Cisco AMP Cloud V1.
2020-10-09	Revision 17: Added Alcide io KAudit, Stormshield Network Security and Tigera Calico
2020-12-18	Revision 18: Added note to AWS CloudTrail API Configuration

Date	Change Description
2021-01-05	Revision 19: Added Mapping Active Directory User Attributes to FortiSIEM User Attributes.
2021-02-03	Revision 20: Updated Malwarebytes to Malwarebytes Endpoint Protection.
2021-03-03	Revision 21: Added NetApp Data ONTAP Supported Version.
2021-03-18	Revision 22: Added Claroty Continuous Threat Detection, Corero Smartwall Threat Defense, Dragos Platform, Malwarebytes Breach Remediation, Oracle Cloud Access Security Broker (CASB), Proofpoint.
2021-04-05	Revision 23: Updated Linux server section.
2021-04-07	Revision 24: Updated AWS Kinesis for 6.2.0.
2021-04-16	Revision 25: Updated Microsoft Office 365 Audit "Create the Office 365 API Credential" steps.
2021-04-23	Revision 26: Added Salesforce Configuration for 6.2.0, 6.1.x, 5.4.0, 5.3.x, 5.2.x releases.
2021-07-06	Revision 27: Added Security Orchestration and FortiGate SNMPv3 setup example. Updated: Cisco Firepower Threat Defense, Linux Server Rsyslog and Syslog-NG, AWS Security Hub, EC2 Cloudwatch API, AWS EC2 Discovery, Office365 API integration, Microsoft Azure Compute, Microsoft Windows Defender for Endpoint (Windows Defender ATP), Cisco IOS, Cisco FireSIGHT, Cisco Duo, Cisco FireAmp, Cisco Meraki Access Points, Rapid7 Nexpose, Rapid7 InsightVM, Google Workspace, Carbon Black Syslog setup, FortiManager syslog, FortiWeb syslog, FortiSandbox syslog, FortiAuthenticator syslog, FortiClient syslog, FortiADC syslog, FortiDeceptor syslog, FortiNAC syslog, FortiEDR syslog, FortiSOAR syslog. Environmental Sensors updated to Operational Technology, Syslog over TLS. New Device Support: Microsoft Windows Print Service Log, AWS Elasticsearch Load Balancer Log, CyberX OT/IoT Security via Log, Digital Defense Vulnerability Scanner via API, FortiAI via Log, FortiCASB integration via API, HP ILO via SNMP Trap, Palo Alto Cortex XDR via Log, Palo Alto WildFire via Log through Palo Alto Firewall. Device Support Extensions: CloudTrail Logs via AWS Kinesis, CyberArk Vault integration via REST API, FortiAnalyzer System Event Logs via Syslog, FortiEDR integration via API, FortiGate, FortiAP and FortiSwitch via FortiGate API, GCC High Tenant for Azure Audit, VPC Flog Logs via AWS Kinesis.
2021-07-22	Revision 28: Updated AWS Kinesis Configuration for Configuring AWS CloudTrail Logs through Kinesis Streams, and Configuring VPC Flow Logs through Kinesis Streams.
2021-07-26	Revision 29: Updated Epilog/snare link for Oracle Database Server, Juniper Steel Belted RADIUS, and Apache Web Server configuration.
2021-07-30	Revision 30: Updated Tenable Nessus Vulnerability Scanner configuration.
2021-08-02	Revision 31: Updated Cisco FireSIGHT Configuration.
2021-08-26	Revision 32: Updated AWS EC2 CloudWatch API, Googe Workspace / GSUITE, Zeek Network Security Monitor (Previously Bro). Added Microsoft Advanced Threat Analytics (ATA) On Premise Platform, KVM, FortiProxy, Google Cloud Platform, Mac OS, Otorio RAM2, UserGate UTM Firewall to 6.3.1.
2021-08-30	Revision 33: Updated Microsoft SQL Server for 6.x Guides.

Date	Change Description
2021-08-31	Revision 34: Added Syslog CEF Format configuration to Check Point FireWall-1 for 6.3.1 Guide.
2021-09-16	Revision 35: Updated Dell Force10 Router and Switch, Dell NSeries Switch, and Dell PowerConnect Switch and Router for 6.3.1, and Microsoft Office 365 Audit for 6.3.x Guides.
2021-09-17	Revision 36: Updated MySQL Server and CyberArk Password Vault for 6.3.x Guides. Added example syslog for Dell Force10 Router and Switch, Dell NSeries Switch, and Dell PowerConnect Switch and Router for 6.3.1 Guide.
2021-09-24	Revision 37: Updated Squid Web Proxy with syslog configuration for versions 4.1.1 and later for 6.1.1-6.3.x Guides.
2021-10-06	Revision 38: Added ArubaOS-CX Switch platform, Barracuda Web Application Firewall, and Cisco Umbrella to 6.3.2 Guide.
2021-10-08	Revision 39: Updated Microsoft Windows Server SNMP Configuration instructions and removed older Microsoft SQL Scripts for 6.3.x.
2021-10-29	Revision 40: Updated Cisco Firepower Management Center (FMC) - Formerly FireSIGHT and FirePower Threat Defense : Using Cisco eStreamer Client for 6.x Guides.
2021-11-01	Revision 41: Updated Configuring FortiSIEM through FortiOS REST API - Step 2: Create an Administrator Profile for 6.3.x.
2021-11-08	Revision 42: Updated Cisco Umbrella Prefix Configuration Information for 6.3.2.
2021-11-16	Revision 43: Updated FortiSIEM External Ports with sFlow port number and protocol from External Devices to Supervisor/Worker/Collector.
2021-11-30	Revision 44: Updated FortiSIEM External Ports Collector Communication table.
2021-12-06	Revision 45: Updated Enable WinRM and set authentication in Microsoft Windows Server.
2021-12-08	Revision 46: Updated Syslog over TLS section for 6.x.
2021-12-23	Revision 47: Google Cloud Platform configuration updated for 6.3.1 and later.
2022-01-06	Revision 48: SNMP V3 Traps section added.

TABLE OF CONTENTS

Overview

This document describes how to configure third party devices for monitoring by FortiSIEM.

- Ports Used by FortiSIEM for Discovery and Monitoring
- Supported Devices and Applications by Vendor
- Windows Agent Installation Guide
- Applications
- Blade Servers
- Cloud Applications
- Console Access Devices
- End Point Security Software
- Firewalls
- Load Balancers and Application Firewalls
- Log Aggregators
- Network Compliance Management Applications
- Network Intrusion Protection Systems (IPS)
- Operational Technology
- Routers and Switches
- Security Gateways
- Servers
- Storage
- Virtualization
- VPN Gateways
- Vulnerability Scanners
- WAN Accelerators
- Wireless LANs
- Using Virtual IPs to Access Devices in Clustered Environments
- Syslog over TLS
- SNMP V3 Traps

FortiSIEM External Ports

This chapter describes the external communication ports needed for various FortiSIEM nodes to work. The ports are broken down for:

- Supervisor Communication
- Worker Communication
- Collector Communication

In release 6.3, some clear communication has been replaced by SSL communication. If an entry in the tables below has 5.3, then that entry is valid for releases 5.3 and below. If an entry in the tables below has 6.3, then that entry is valid for releases 6.3 and above.

Supervisor Communication

From	To	Inbound or Outbound	Ports	Services
FortiSIEM Management User	Supervisor	Inbound	TCP/22	Admin access via SSH
FortiSIEM Management User	Supervisor	Inbound	ICMP	Monitoring via ICMP
FortiSIEM Management User	Supervisor	Inbound	TCP/443	GUI access via HTTPS
Collector, Worker, Windows Agent, Linux Agent	Supervisor	Inbound	TCP/443	REST API access via HTTPS
Supervisor	Report Server	Outbound	TCP/5432	PostGreSQL (report loading)
Worker	Supervisor	Inbound	SSL/7914	phParser on Worker to phParser on Supervisor for EPS enforcement
Worker	Supervisor	Inbound	SSL/7900	phMonitorWorker to phMonitorSuper communication
Supervisor	Worker	Outbound	SSL/7900	phMonitorSuper to phMonitorWorker Communication
Worker	Supervisor	Inbound	SSL/7918	phQueryWorker to phQueryMaster Communication

From	To	Inbound or Outbound	Ports	Services
Supervisor	Worker	Outbound	SSL/7916	phQueryMaster to phQueryWorker communication
Worker	Supervisor	Inbound	SSL/7922	phRuleWorker to phRuleMaster communication
Worker 6.1	Supervisor	Outbound	SSL/7920	phQueryMaster to phDataManager for trigger event query
Worker	Supervisor	Inbound	SSL/7934	phReportWorker to phReportMaster Communication
Worker	Supervisor	Inbound	SSL/7938	phIdentityWorker to phIpIdentityMaster
Supervisor	Worker	Outbound	TCP/6666	Redis communication
Worker	Supervisor	Inbound	TCP/5555	phFortiInsightAI module data collection
Supervisor	External Device	Outbound	UDP/161	SNMP based monitoring
External Device	Supervisor	Inbound	TCP/21	FTP (for receiving Bluecoat logs via ftp)
External Device	Supervisor	Inbound	UDP/162	SNMP Trap
External Device	Supervisor	Inbound	UDP/514	UDP syslog
External Device	Supervisor	Inbound	TCP/514	TCP syslog
External Device	Supervisor	Inbound	SSL/6514	Syslog over TLS
External Device	Supervisor	Inbound	UDP/2055	NetFlow
External Device	Supervisor	Inbound	UDP/6343	sFlow
Supervisor	External Windows Devices	Outbound	TCP/135	WMI based monitoring and log collection
Supervisor	External Devices	Outbound	TCP/389	LDAP discovery
Supervisor	External Devices	Outbound	TCP/1433	JDBC based monitoring and data collection
Supervisor	External Devices	Outbound	UDP/8686	JMX based monitoring and data collection
Supervisor	Checkpoint	Outbound	TCP/18184	Checkpoint LEA based log collection

From	To	Inbound or Outbound	Ports	Services
Supervisor	Checkpoint	Outbound	TCP/18190	Checkpoint CPMI based data collection
Supervisor	External Device	Outbound	TCP/443	HTTPS based log collection
Supervisor	External Device	Outbound	TCP/110	POP3 for email monitoring (STM)
Supervisor	External Device	Outbound	TCP/143	IMAP for email monitoring (STM)
Supervisor	External Device	Outbound	TCP/993	IMAP/SSL for email monitoring (STM)
Supervisor	External Device	Outbound	TCP/995	POP/SSL for email monitoring (STM)
Supervisor	Mail Gateway	Outbound	TCP/SMTP	Sending email notification
Supervisor	NFS Server	Outbound	UDP/111, TCP/111	NFS Portmapper for writing events in NFS based deployments
Supervisor	Elasticsearch Coordinating Node	Outbound	HTTPS/9200 (configurable)	Storing events for Elasticsearch based deployments
Supervisor	Elasticsearch Coordinating Node	Outbound	HTTPS/9300 or HTTPS/443 (configurable)	Querying events for Elasticsearch based deployments
Supervisor	Spark Master Node	Outbound	HTTPS/7077 (configurable)	Querying events for HDFS based deployments
Supervisor	HDFS Name Node	Outbound	HTTPS/9000 (configurable)	Archiving events for HDFS based deployments

Worker Communication

From	To	Inbound or Outbound	Ports	Services
FortiSIEM Management User	Worker	Inbound	TCP/22	Admin access via SSH

From	To	Inbound or Outbound	Ports	Services
FortiSIEM Management User	Worker	Inbound	ICMP	ICMP
Collector	Worker	Inbound	TCP/443	REST API access via HTTPS
Worker	Supervisor	Outbound	SSL/7914	phParser on Worker to phParser on Supervisor for EPS enforcement
Worker	Supervisor	Outbound	SSL/7900	phMonitorWorker to phMonitorSuper communication
Supervisor	Worker	Inbound	SSL/7900	phMonitorSuper to phMonitorWorker Communication
Worker	Supervisor	Outbound	SSL/7918	phQueryWorker to phQueryMaster Communication
Supervisor	Worker	Inbound	SSL/7916	phQueryMaster to phQueryWorker communication
Worker	Supervisor	Outbound	SSL/7922	phRuleWorker to phRuleMaster communication
Worker 6.1	Supervisor	Outbound	SSL/7920	phQueryMaster to phDataManager for trigger event query
Worker	Supervisor	Outbound	SSL/7934	phReportWorker to phReportMaster Communication
Worker	Supervisor	Outbound	SSL/7938	phIdentityWorker to phIpIdentityMaster
Supervisor	Worker	Inbound	TCP/6666	Redis communication
Worker	Supervisor	Outbound	TCP/5555	phFortiInsightAI module data collection
Worker	External Device	Outbound	UDP/161	SNMP based monitoring
External Device	Worker	Inbound	TCP/21	FTP (for receiving Bluecoat logs via ftp)
External Device	Worker	Inbound	UDP/162	SNMP Trap
External Device	Worker	Inbound	UDP/514	UDP syslog
External Device	Worker	Inbound	TCP/514	TCP syslog
External Device	Worker	Inbound	SSL/6514	Syslog over TLS
External Device	Worker	Inbound	UDP/2055	NetFlow
External Device	Worker	Inbound	UDP/6343	sFlow
Worker	External Windows Devices	Outbound	TCP/135	WMI based monitoring and log collection
Worker	External Devices	Outbound	TCP/389	LDAP discovery

From	To	Inbound or Outbound	Ports	Services
Worker	External Devices	Outbound	TCP/1433	JDBC based monitoring and data collection
Worker	External Devices	Outbound	UDP/8686	JMX based monitoring and data collection
Worker	Checkpoint	Outbound	TCP/18184	Checkpoint LEA based log collection
Worker	Checkpoint	Outbound	TCP/18190	Checkpoint CPMI based data collection
Worker	External Device	Outbound	TCP/443	HTTPS based log collection
Worker	External Device	Outbound	TCP/110	POP3 for email monitoring (STM)
Worker	External Device	Outbound	TCP/143	IMAP for email monitoring (STM)
Worker	External Device	Outbound	TCP/993	IMAP/SSL for email monitoring (STM)
Worker	External Device	Outbound	TCP/995	POP/SSL for email monitoring (STM)
Worker	NFS Server	Outbound	UDP/111, TCP/111	NFS Portmapper for writing events in NFS based deployments
Worker	Elasticsearch Coordinating Node	Outbound	HTTPS/9200 (configurable)	Storing events for Elasticsearch based deployments
Worker	HDFS Name Node	Outbound	HTTPS/9000 (configurable)	Archiving events for HDFS based deployments

Collector Communication

From	To	Inbound or Outbound	Ports	Services
FortiSIEM Management User	Collector	Inbound	TCP/22	Admin access via SSH
FortiSIEM Management User	Collector	Inbound	ICMP	ICMP
Collector	Collector	Outbound	TCP/443	REST API access via HTTPS
Collector	Supervisor	Outbound	TCP/443	REST API access via HTTPS
Collector	External Device	Outbound	UDP/161	SNMP based monitoring
External Device	Collector	Inbound	TCP/21	FTP (for receiving Bluecoat logs via ftp)
External Device	Collector	Inbound	UDP/162	SNMP Trap

From	To	Inbound or Outbound	Ports	Services
External Device	Collector	Inbound	UDP/514	UDP syslog
External Device	Collector	Inbound	TCP/514	TCP syslog
External Device	Collector	Inbound	SSL/6514	Syslog over TLS
External Device	Collector	Inbound	UDP/2055	NetFlow
External Device	Collector	Inbound	UDP/6343	sFlow
Collector	External Windows Devices	Outbound	TCP/135	WMI based monitoring and log collection
Collector	External Devices	Outbound	TCP/389	LDAP discovery
Collector	External Devices	Outbound	TCP/1433	JDBC based monitoring and data collection
Collector	External Devices	Outbound	UDP/8686	JMX based monitoring and data collection
Collector	Checkpoint	Outbound	TCP/18184	Checkpoint LEA based log collection
Collector	Checkpoint	Outbound	TCP/18190	Checkpoint CPMI based data collection
Collector	External Device	Outbound	TCP/443	HTTPS based log collection
Collector	External Device	Outbound	TCP/110	POP3 for email monitoring (STM)
Collector	External Device	Outbound	TCP/143	IMAP for email monitoring (STM)
Collector	External Device	Outbound	TCP/993	IMAP/SSL for email monitoring (STM)
Collector	External Device	Outbound	TCP/995	POP/SSL for email monitoring (STM)

Supported Devices and Applications by Vendor

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
AirTight Networks	SpectraGuard	Discovered via LOG only	Not natively supported - Custom monitoring needed	CEF format: Over 125 event types parsed covering various Wireless suspicious activities	Currently not natively supported	AirTight Networks SpectraGuard
Alcatel	TiMOS Routers and Switches	SNMP: OS, Hardware	SNMP: CPU, memory, interface utilization, hardware status	Not natively supported - Custom parsing needed	Currently not natively supported	Alcatel TiMOS and AOS Switch Configuration
Alcatel	AOS Routers and Switches	SNMP: OS, Hardware	SNMP: CPU, memory, interface utilization, hardware status	Not natively supported - Custom parsing needed	Currently not natively supported	Alcatel TiMOS and AOS Switch Configuration
Alert Logic	Intrusion Detection and Prevention Systems (IPS)	Host name and Device type	Not supported		Not supported	Alert Logic IPS
Alert Logic	Iris API	Host name and Device type	Not supported		Not supported	Alert Logic IRIS API
Alcide.io	KAudit	Not natively supported	Not natively supported	Kubernetes Audit logs	Not natively supported	Alcide io KAudit
Amazon	AWS Servers	AWS API: Server Name, Access IP, Instance ID, Image Type, Availability Zone	CloudWatch API: System Metrics: CPU, Disk I/O, Network	CloudTrail API: Over 325 event types parsed covering various AWS activities	CloudTrail API: various administrative changes on AWS systems and users	AWS CloudWatchAWS CloudTrail
Amazon	AWS Elastic Block Storage (EBS)	CloudWatch API: Volume ID, Status, Attach Time	CloudWatch API: Read/Write Bytes, Ops, Disk Queue			AWS EBS and RDS
Amazon	AWS EC2					AWS EC2
Amazon	AWS Elastic Load Balancer (ELB)					AWS ELB
Amazon	AWS Relational Database Storage		CloudWatch API: CPU, Connections, Memory, Swap,			AWS EBS and RDS

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	(RDS)		Read/Write Latency and Ops			
Amazon	Security Hub					AWS Security Hub
Apache	Tomcat Application Server	JMX: Version	JMX: CPU, memory, servlet, session, database, threadpool, request processor metrics	Currently not natively supported - Custom parsing needed	Currently not natively supported	Apache Tomcat
Apache	Apache Web server	SNMP: Process name	SNMP: process level cpu, memory HTTPS via the mod-status module: Apache level metrics	Syslog: W3C formatted access logs - per HTTP (S) connection: Sent Bytes, Received Bytes, Connection Duration	Currently not natively supported	Apache Web Server
APC	NetBotz Environmental Monitor	SNMP: Host name, Hardware model, Network interfaces	SNMP: Temperature, Relative Humidity, Airflow, Dew point, Current, Door switch sensor etc.	SNMP Trap: Over 125 SNMP Trap event types parsed covering various environmental exception conditions	Currently not natively supported	APC Netbotz
APC	UPS	SNMP: Host name, Hardware model, Network interfaces	SNMP: UPS metrics	SNMP Trap: Over 49 SNMP Trap event types parsed covering various environmental exception conditions	Currently not natively supported	APC UPS
Arista Networks	Routers and Switches	SNMP: OS, Hardwar; SSH: configuration, running processes	SNMP: CPU, Memory, Interface utilization, Hardware Status	Syslog and NetFlow	SSH: Running config, Startup config	Arista Router and Switch
Aruba Networks	Aruba Wireless LAN	SNMP: Controller OS, hardware, Access Points	SNMP: Controller CPU, Memory, Interface utilization, Hardware Status SNMP: Access Point Wireless Channel utilization, noise metrics, user count	SNMP Trap: Over 165 event types covering Authentication, Association, Rogue detection, Wireless IPS events	Currently not natively supported	Aruba WLAN
Avaya	Call Manager	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status	CDR: Call Records	Currently not natively supported	Avaya Call Manager
Avaya	Session Manager	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		Currently not natively supported	

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Barracuda Networks	Spam Firewall	Application type discovery via LOG	Currently not natively supported	Syslog: Over 20 event types covering mail scanning and filtering activity	Currently not natively supported	Barracuda Spam
Bit9	Security platform	Application type discovery via LOG	Currently not natively supported	Syslog: Over 259 event types covering various file monitoring activities	Currently not natively supported	Bit9 Security Platform
Blue Coat	Security Gateway Versions v4.x and later	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Proxy performance metrics	Syslog: Admin access to Security Gateway ; SFTP: Proxy traffic analysis	Currently not natively supported	Blue Coat Web Proxy
Box.com	Cloud Storage	Currently not natively supported	Currently not natively supported	Box.com API: File creation, deletion, modify, file sharing	Currently not natively supported	Box.com
Brocade	SAN Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	Currently not natively supported	Currently not natively supported	Brocade SAN Switch
Brocade	ServerIron ADX switch	SNMP: Host name, serial number, hardware	SNMP: Uptime, CPU, Memory, Interface Utilization, Hardware status, Real Server Statistics			Brocade ADX
Carbon Black	Security platform	Application type discovery via LOG	Currently not natively supported	Syslog: Over 259 event types covering various file monitoring activities	Currently not natively supported	Carbon Black Security Platform
CentOS / Other Linux distributions	Linux	SNMP: OS, Hardware, Software, Processes, Open Ports SSH: Hardware details, Linux distribution	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification; SSH: File integrity monitoring, Command output monitoring, Target file monitoring; FortiSIEM LinuxFileMon Agent: File integrity monitoring	SSH: File integrity monitoring, Target file monitoring; Agent: File integrity monitoring	Linux Server
CentOS / Other Linux distributions	DHCP Server	Currently not natively supported	Currently not natively supported	Syslog: DHCP activity (Discover, Offer, Request, Release etc) - Used in Identity and Location	Not Applicable	Linux DHCP

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Checkpoint	FireWall-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX,R75, R80	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	LEA from SmartCenter or Log Server: Firewall Log, Audit trail, over 940 IPS Signatures	LEA: Firewall Audit trail	Check Point Provider-1 Firewall
Checkpoint	GAIA	Host name and Device type		Over 9 event types		
Checkpoint	Provider-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, and R75	Currently not natively supported	Currently not natively supported	LEA: Firewall Log, Audit trail	LEA: Firewall Audit trail	Check Point Provider-1
Checkpoint	VSX	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	LEA from SmartCenter or Log Server: Firewall Log, Audit trail	LEA: Firewall Audit trail	Check Point Provider-1
Citrix	NetScaler Application Delivery Controller	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status, Application Firewall metrics	Syslog: Over 465 event types covering admin activity, application firewall events, health events	Currently not natively supported	Citrix Netscaler
Citrix	ICA	SNMP: Process Utilization	SNMP: Process Utilization; WMI: ICA Session metrics	Currently not natively supported	Currently not natively supported	Citrix ICA
Cisco	ASA Firewall (single and multi-context) version 7.x and later	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Firewall Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity; NetFlow V9: Traffic log	SSH: Running config, Startup config	Cisco ASA
Cisco	AMP					Cisco AMP for Endpoints API V1 - Previously Cisco AMP
Cisco	FireAMP					Cisco AMP for Endpoints API V0 - Previously Cisco

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
						FireAMP Cloud
Cisco	ASA firepower SFR Module	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Firewall Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity; NetFlow V9: Traffic log	SSH: Running config, Startup config	Cisco ASA
Cisco	Firepower Threat Defense					Cisco FTD
Cisco	CatOS based Switches	SNMP: OS, Hardware (Serial Number, Image file, Interfaces, Components); SSH: configuration running process	SNMP: CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 700 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, IPS activity NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config	Cisco IOS
Cisco	Duo		Not natively supported - Custom Monitoring needed	Via API	Not natively supported - Custom Custom Configuration collection needed	Cisco Duo
Cisco	PIX Firewall	SNMP: OS, Hardware SSH: interface security level needed for parsing traffic logs, Configuration	SNMP: CPU, Memory, Interface utilization, Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering admin access, configuration change, traffic log, IPS activity	SSH: Running config, Startup config	Cisco ASA
Cisco	FWSM	SNMP: OS, Hardware SSH:	SNMP: CPU, Memory, Interface utilization, Connections, Hardware Status	Syslog: Over 1600 event types parsed for situations covering	SSH: Running config,	Cisco ASA

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		interface security level needed for parsing traffic logs, Configuration		admin access, configuration change, traffic log, IPS activity	Startup config	
Cisco	Identity Services Engine (ISE)	Host name and Device type				Cisco ISE
Cisco	IOS based Routers and Switches	SNMP: OS, Hardware; SSH: configuration, running process, Layer 2 connectivity	SNMP: CPU, Memory, Interface utilization, Hardware Status; SNMP: IP SLA metrics; SNMP: BGP metrics, OSPF metrics; SNMP: Class based QoS metrics; SNMP: NBAR metrics	Syslog: Over 200 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, IPS activity; NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config	Cisco IOS
Cisco	Nexus OS based Routers and Switches	SNMP: OS, Hardware; SSH: configuration running process, Layer 2 connectivity	SNMP: CPU, Memory, Interface utilization, Hardware Status; SNMP: IP SLA metrics, BGP metrics, OSPF metrics, NBAR metrics; SNMP: Class based QoS metrics	Syslog: Over 3500 event types parsed for situations covering admin access, configuration change, interface up/down, BGP interface up/down, traffic log, hardware status, software and hardware errors; NetFlow V5, V9: Traffic logs	SSH: Running config, Startup config	Cisco NX-OS
Cisco	ONS	SNMP: OS, Hardware		SNMP Trap: Availability and Performance Alerts		Cisco NX-OS
Cisco	ACE Application Firewall	SNMP: OS, Hardware				
Cisco	UCS Server	UCS API: Hardware components - processors, chassis, blades, board, cpu, memory, storage,	UCS API: Chassis Status, Memory Status, Processor Status, Power Supply status, Fan status	Syslog: Over 500 event types parsed for situations covering hardware errors, internal software errors etc	Currently not natively supported	Cisco UCS

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		power supply unit, fan unit				
Cisco	WLAN Controller and Access Points	SNMP: OS, Hardware, Access Points	SNMP: Controller CPU, Memory, Interface utilization, Hardware Status; SNMP: Access Point Wireless Channel utilization, noise metrics, user count	SNMP Trap: Over 88 event types parsed for situations covering Authentication, Association, Rogue detection, Wireless IPS events	Currently not natively supported	Cisco Wireless LAN
Cisco	Call Manager	SNMP: OS, Hardware, VoIP Phones	SNMP: Call manager CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage; SNMP: VoIP phone count, Gateway count, Media Device count, Voice mail server count and SIP Trunks count; SNMP: SIP Trunk Info, Gateway Status Info, H323 Device Info, Voice Mail Device Info, Media Device Info, Computer Telephony Integration (CTI) Device Info	Syslog: Over 950 messages from Cisco Call Manager as well as Cisco Unified Real Time Monitoring Tool (RTMT); CDR Records, CMR Records: Call Source and Destination, Time, Call Quality metrics (MOS Score, Jitter, latency)	Currently not natively supported	Cisco Call Manager
Cisco	Contact Center	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Contact Center
Cisco	Presence Server	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Presence Server
Cisco	Tandeberg Tele-presence Video Communication Server (VCS)	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Tandeberg Telepresence VCS
Cisco	Tandeberg Tele-presence Multiple Control Unit (MCU)	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Telepresence MCU
Cisco	Unity Connection	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Unity

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Cisco	IronPort Mail Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	Syslog: Over 45 event types covering mail scanning and forwarding status	Currently not natively supported	Cisco IronPort Mail
Cisco	IronPort Web Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status, Process level resource usage, Install software change	W3C Access log (Syslog): Over 9 event types covering web request handling status	Currently not natively supported	Cisco IronPort Web
Cisco	Cisco Network IPS Appliances	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk Interface utilization, Hardware Status	SDEE: Over 8000 IPS signatures	Currently not natively supported	Cisco NIPS
Cisco	Sourcefire 3D and Defense Center	SNMP: OS, Hardware				Sourcefire 3D and Defense Center
Cisco	Cisco Firepower Management Center (FMC) - Previously FireSIGHT Console			eStreamer SDK: Intrusion events, Malware events, File events, Discovery events, User activity events, Impact flag events		Cisco Firepower Management Center (FMC) - Previously Cisco FireSIGHT
Cisco	Cisco Security Agent	SNMP or WMI: OS, Hardware	SNMP or WMI: Process CPU and memory utilization	SNMP Trap: Over 25 event types covering Host IPS behavioral signatures.	Currently not natively supported	Cisco CSA
Cisco	Cisco Access Control Server (ACS)	SNMP or WMI: OS, Hardware	SNMP or WMI: Process CPU and memory utilization	Syslog: Passed and Failed authentications, Admin accesses	Currently not natively supported	Cisco ACS
Cisco	VPN 3000	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization	Syslog: Successful and Failed Admin Authentication, VPN Authentication, IPSec Phase 1 and Phase 2 association, VPN statistics	Currently not natively supported	Cisco VPN 3000
Cisco	Meraki Cloud Controllers	SNMP: OS, Hardware, Meraki devices reporting to the Cloud Controller	SNMP: Uptime, Network Interface Utilization; SNMP Trap: Various availability scenarios	Currently not natively supported - Custom parsing needed	Currently not natively supported	Cisco Meraki Cloud Controller and Network Devices

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Cisco	Meraki Firewalls	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization	Syslog: Firewall log analysis	Currently not natively supported	Cisco Meraki Cloud Controller and Network Devices
Cisco	Meraki Routers/Switches	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization		Currently not natively supported	Cisco Meraki Cloud Controller and Network Devices
Cisco	Meraki WLAN Access Points	SNMP: OS, Hardware	SNMP: Uptime, Network Interface Utilization		Currently not natively supported	Cisco Meraki Cloud Controller and Network Devices
Cisco	MDS Storage Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status	Currently not natively supported - Custom parsing needed	Currently not natively supported	
Cisco	Network Control Manager (NCM)			Syslog: Network device software update, configuration analysis for compliance, admin login		Cisco Network Compliance Manager
Cisco	Stealthwatch	Host name and Device type	Not supported		Not supported	Cisco Stealthwatch
Cisco	Umbrella			DNS logs, Proxy logs, IP logs, Admin Audit logs		Cisco Umbrella
Cisco	Viptela	Discovered Via LOG only	Not natively supported - Custom monitoring needed	Over 289 Events Types parsed	Not natively supported - Custom configuration collection needed	Cisco Viptela SDWAN Router
Cisco	Wide Area Application Services (WAAS)	SNMP: Host name, Version, Hardware model, Network interfaces	SNMP: CPU, Memory, Interface utilization, Disk utilization, Process cpu/memory utilization			Cisco WAAS
Claroty	Continuous Threat Detection					Claroty Continuous

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	(CTD)					Threat Detection (CTD)
CloudPassage	Halo	Host name and Device type	Not supported		Not supported	CloudPassage Halo
Corero	Smartwall Threat Defense System					Corero Smartwall Threat Defense System
CradlePoint	CradlePoint	Discovered via LOG only	Not natively supported. Custom monitoring needed	29 Event types covering Security Violations, Config Changes, Authentications and informational events	Not currently supported.	CradlePoint
CrowdStrike	Falcon	Host name and Device type	Not supported		Not supported	CrowdStrike Falcon
Cyberoam	Cyberoam	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Event, Security, and Traffic logs	Connection - permit and deny, system events, maleware events	Cyberoam Firewall
Cylance	Cylance Protect Endpoint Protection			Syslog: Endpoint protection alerts		Cylance Protect
Cyphort	Cyphort Cortex Endpoint Protection			Syslog: Endpoint protection alerts		Cyphort Cortex
Cyxtera	AppGate SDP	Host name and Device type	Not supported		Not supported	Cyxtera AppGate SDP
Damballa	Failsafe					Damballa Failsafe
Darktrace	CyberIntelligence Platform	Discovered via LOG only	Not natively supported - Custom monitoring needed	Over 40 Events Types parsed	Not Natively Supported - Custom Configuration collection needed	Darktrace CyberIntelligence Platform
Dell	SonicWall Firewall	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Firewall session count	Syslog: Firewall log analysis (over 1000	Currently not natively	Dell SonicWALL

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				event types)	supported	
Dell	Force10 Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Interface Status, Hardware Status		SSH: Running config, Startup config	Dell Force10
Dell	NSeries Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		SSH: Startup config	Dell NSeries
Dell	PowerConnect Router and Switch	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Hardware Status		SSH: Startup config	Dell PowerConnect
Dell	Dell Hardware on Intel-based Servers	SNMP: Hardware	SNMP: Hardware Status: Battery, Disk, Memory, Power supply, Temperature, Fan, Amperage, Voltage		Currently not natively supported.	
Dell	Compellent Storage	SNMP: OS, Hardware	SNMP: Network Interface utilization, Volume utilization, Hardware Status (Power, Temperature, Fan)		Currently not natively supported.	Dell Compellent
Dell	EqualLogic Storage	SNMP: OS, Hardware (Network interfaces, Physical Disks, Components)	SNMP: Uptime, Network Interface utilization; SNMP: Hardware status: Disk, Power supply, Temperature, Fan, RAID health; SNMP: Overall Disk health metrics**:** Total disk count, Active disk count, Failed disk count, Spare disk count; SNMP: Connection metrics: IOPS, Throughput; SNMP: Disk performance metrics: IOPS, Throughput; SNMP: Group level performance metrics: Storage, Snapshot		Currently not natively supported.	Dell EqualLogic
Digital Defense	Frontline Vulnerability Manager			Frontline API: Host name, Vulnerability name, Vulnerability CVE ID, Vulnerability score, and operating system in event.		Digital Defense Frontline Vulnerability Manager
Digital Guardian	Code Green DLP	LOG Discovery	Currently not natively supported	1 broad event Type	Currently not natively supported	Digital Guardian Code Green DLP

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Dragos	Platform - Industrial control systems (ICS) and OT (operational technology)					Dragos Platform
EMC	Clariion Storage	Naviseccli: Host name, Operating system version, Hardware model, Serial number, Network interfaces, Installed Software, Storage Controller Ports; Naviseccli: Hardware components, RAID Groups and assigned disks, LUNs and LUN -> RAID Group mappings, Storage Groups and memberships	Naviseccli: Storage Processor utilization, Storage Port I/O, RAID Group I/O, LUN I/O, Host HBA Connectivity, Host HBA Unregistered Host, Hardware component health, Overall Disk health, Storage Pool Utilization		Currently not natively supported.	EMC Clariion
EMC	VNX Storage	Naviseccli: Host name, Operating system version, Hardware model, Serial number, Network interfaces,	Naviseccli: Storage Processor utilization, Storage Port I/O, RAID Group I/O, LUN I/O, Host HBA Connectivity, Host HBA Unregistered Host, Hardware component health, Overall Disk health, Storage Pool Utilization			EMC VNX

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		Installed Software, Storage Controller Ports Naviseccli: Hardware components, RAID Groups and assigned disks, LUNs and LUN -> RAID Group mappings, Storage Groups and memberships				
EMC	Isilon Storage	SNMP: Host name, Operating system, Hardware (Model, Serial number, Network interfaces, Physical Disks, Components)	SNMP: Uptime, Network Interface metrics; SNMP: Hardware component health: Disk, Power supply, Temperature, Fan, Voltage; SNMP: Cluster membership change, Node health and performance (CPU, I/O), Cluster health and performance, Cluster Snapshot, Storage Quota metrics, Disk performance, Protocol performance	5 event types		EMC Isilon
Epic	SecuritySIEM	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Authentication Query, Client login Query	Currently not natively supported	Epic EMR/EHR System
ESET	Nod32 Anti-virus	Application type discovery via LOG		Syslog (CEF format): Virus found/cleaned type of events		ESET NOD32
FireEye	Malware Protection System (MPS)	Application type discovery via LOG		Syslog (CEF format): Malware found/cleaned type of events		FireEye MPS
FireEye	HX Appliances for Endpoint protection	Application type discovery via LOG		Syslog (CEF format): Malware Acquisition, Containment type of events		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
F5 Networks	Application Security Manager	Discovery via LOG		Syslog (CEF Format); Various application level attack scenarios - invalid directory access, SQL injections, cross site exploits		F5 Application Security Manager
F5 Networks	Local Traffic Manager	SNMP: Host name, Operating system, Hardware (Model, Serial number, Network interfaces, Physical Disks), Installed Software, Running Software	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start	SNMP Trap: Exception situations including hardware failures, certain security attacks, Policy violations etc; Syslog: Permitted and Denied Traffic		F5 Networks Local Traffic Manager
F5 Networks	Web Accelerator	Discovery via LOG		Syslog: Permitted Traffic		F5 Networks Web Accelerator
Fortinet	FortiAnalyzer					Fortinet FortiAnalyzer
Fortinet	FortiAP	Access point – Name, OS, Interfaces, Controller (FortiGate)	FortiAP CPU, Memory, Clients, Sent/Received traffic	Wireless events via FortiGate		FortiAP
Fortinet	FortiAuthenticator	Vendor, OS, Model	Interface Stat, Authentication Stat	Over 150 event types	Currently not natively supported.	Fortinet FortiAuthenticator
Fortinet	FortiClient	Discovered via LOG only		Syslog: Traffic logs, Event logs	Not supported	FortiClient
Fortinet	FortiDeceptor	Discovered via LOG only	Not natively supported. Custom monitoring needed.	Authentication logs, Decoy activity	Currently not natively supported.	Fortinet FortiDeceptor
Fortinet	FortiEDR	Discovered via LOG only	Not natively supported. Custom monitoring needed.	System and security events (e.g. file blocked)	Currently not natively supported	Fortinet FortiEDR

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Fortinet	FortiGate firewalls	SNMP: OS, Host name, Hardware (Serial Number, Interfaces, Components)	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics	Syslog: Over 11000 Traffic and system logs; Netflow: traffic flow, Application flow	SSH: Running config, Startup config	Fortinet FortiGate
Fortinet	FortiInsight					FortiInsight
Fortinet	FortiManager	SNMP: Host name, Hardware model, Network interfaces, Operating system version	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics			FortiManager
Fortinet	FortiNAC	Discovered via LOG only	Not natively supported. Custom monitoring needed	Administrative and User Admission Control events	Currently not natively supported	Fortinet FortiNAC
Fortinet	FortiWLC	SNMP - Controller – Name, OS, Serial Number, Interfaces, Associated Access Points – name, OS, Interfaces	Controller – CPU, Memory, Disk, Throughput, QoS statistics, Station count	Hardware/Software errors, failures, logons, license expiry, Access Point Association / Disassociation	Not supported	FortiWLC
Fortinet	FortiTester	Discovered Via LOG only	Not natively supported - Custom monitoring needed	CEF format: Over 14 Event types parsed	Not natively supported - Custom configuration collection needed	Fortinet FortiTester
Foundry Networks	IronWare Router and Switch	SNMP: OS, Hardware SSH: configuration, running process	SNMP: Uptime, CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 6000 event types parsed for situations covering admin access, configuration change, interface up/down	SSH: Running config, Startup config	Foundry Networks IronWare

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
FreeBSD						
GitHub.com	GitHub	Host name and Device type	Not supported		Not supported	GitHub
GitLab API	GitLab	Host name and Device type	Not supported		Not supported	GitLab API
GitLab CLI	GitLab	Host name and Device type	Not supported		Not supported	GitLab CLI
Green League	WVSS					Green League WVSS
Huawei	VRP Router and Switch	SNMP: OS, Hardware; SSH: configuration, running process, Layer 2 connectivity	SNMP: Uptime, CPU, Memory, Interface utilization, Hardware Status	Syslog: Over 30 event types parsed for situations covering admin access, configuration change, interface up/down	SSH: Running config, Startup config	
HP	BladeSystem	SNMP: Host name, Access IP, Hardware components	SNMP: hardware status			HP BladeSystem
HP	HP-UX servers	SNMP: OS, Hardware	SNMP: Uptime, CPU, Memory, Network Interface, Disk space utilization, Network Interface Errors, Running Process Count, Running process CPU/memory utilization, Running process start/stop; SNMP: Installed Software change; SSH : Memory paging rate, Disk I/O utilization			HP UX Server
HP	HP Hardware on Intel-based Servers	SNMP: hardware model, hardware serial, hardware components (fan, power	SNMP: hardware status	SNMP Trap: Over 100 traps covering hardware issues		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		supply, battery, raid, disk, memory)				
HP	TippingPoint UnityOne IPS	SNMP: OS, Hardware	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors	Syslog: Over 4900 IPS alerts directly or via NMS		TippingPoint IPS
HP	ProCurve Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors; SNMP: hardware status		SSH: Running config, Startup config	HP ProCurve
HP	Value Series (19xx) Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors		SSH: Startup config	HP Value Series (19xx) and HP 3Com (29xx) Switch
HP	3Com (29xx) Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors		SSH: Startup config	HP Value Series (19xx) and HP 3Com (29xx) Switch
HP	HP/3Com Comware Switches and Routers	SNMP: OS, hardware model, hardware serial, hardware components; SSH: configuration	SNMP: Uptime, CPU, Memory, Network Interface, Network Interface Errors; SNMP: hardware status	Syslog: Over 6000 vent types parsed for situations covering admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup config	HP/3Com ComWare

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Hirschmann	Switches	Host Name, OS	SNMP – Uptime, CPU, Memory, Interface utilization, hardware Status, OSPF metrics	Not natively supported - Custom parsing needed	Not natively supported - Custom configuration collection needed	Hirschmann SCADA Firfewalls and Switches
HyTrust	CloudControl	LOG Discovery	Currently not natively supported	Over 70 event types	Currently not natively supported	HyTrust CloudControl
IBM	Websphere Application Server	SNMP or WMI: Running processes	HTTP(S): Generic Information, Availability metrics, CPU / Memory metrics, Servlet metrics, Database pool metrics, Thread pool metrics, Application level metrics, EJB metrics			IBM WebSphere
IBM	DB2 Database Server	SNMP or WMI: Running processes	JDBC: Database Audit trail: Log on, Database level and Table level CREATE/DELETE/MODIFY operations			IBM DB2
IBM	ISS Proventia IPS Appliances			SNMP Trap: IPS Alerts: Over 3500 event types		IBM ISS Proventia
IBM	AIX Servers	SNMP: OS, Hardware, Installed Software, Running Processes, Open Ports; SSH: Hardware details	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: General logs including Authentication Success/Failure, Privileged logons, User/Group Modification		IBM AIX
IBM	OS 400			Syslog via PowerTech Agent: Over 560 event types		IBM OS400
Imperva	Securesphere DB Monitoring Gateway					Imperva Securesphere DB Monitoring Gateway
Imperva	Securesphere DB Security Gateway			Syslog in CEF format		Imperva Securesphere DB Security Gateway

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Imperva	Securesphere Web App Firewall					Imperva SecureSphere Web App Firewall
Indegy	Security Platform	Discovered via LOG only	Not natively supported - Custom monitoring needed	Over 14 Events Types parsed	Not natively supported - Custom configuration collection needed	Indegy Security Platform
Intel/McAfee	McAfee Sidewinder Firewall	SNMP: OS, Hardware, Installed Software, Running Processes	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start	Syslog: Firewall logs		McAfee Firewall Enterprise (Sidewinder)
Intel/McAfee	McAfee ePO	SNMP: Related process name and parameters	SNMP: Process resource utilization	SNMP Trap: Over 170 event types		McAfee ePolicy Orchestrator (ePO)
Intel/McAfee	Intrushield IPS	SNMP: OS, Hardware	SNMP: Hardware status	Syslog: IPS Alerts		McAfee IntruShield
Intel/McAfee	Stonesoft IPS			Syslog: IPS Alerts		McAfee Stonesoft
Intel/McAfee	Web Gateway			Syslog: Web server log		McAfee Web Gateway
Intel/McAfee	Foundstone Vulnerability Scanner			JDBC: Vulnerability data		McAfee Foundstone Vulnerability Scanner
Infoblox	DNS/DHCP Appliance	SNMP: OS, Hardware, Installed Software, Running Processes	; SNMP: Zone transfer metrics, DNS Cluster Replication metrics, DNS Performance metrics, DHCP Performance metrics, DDNS Update metrics, DHCP subnet usage metrics ; SNMP: Hardware Status ; SNMP Trap: Hardware/Software Errors	Syslog: DNS logs - name resolution activity - success and failures		Infoblox DNS/DHCP
ISC	Bind DNS			Syslog: DNS logs - name resolution activity - success and failures		ISC BIND DNS

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Juniper	JunOS Router/Switch	SNMP: OS, Hardware; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status ;	Syslog: Over 1420 event types parsed for situations covering admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks JunOS
Juniper	SRX Firewalls	SNMP: OS, Hardware SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 700 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks JunOS
Juniper	SSG Firewall	SNMP: OS, Hardware ; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 40 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks SSG Firewall
Juniper	ISG Firewall	SNMP: OS, Hardware ; SSH: Configuration	SNMP: CPU, Memory, Disk, Interface utilization, Hardware Status	Syslog: Over 40 event types parsed for situations covering traffic log, admin access, configuration change, interface up/down and other hardware issues and internal errors	SSH: Startup configuration	Juniper Networks SSG Firewall
Juniper	Steel-belted Radius	Discovered via LOG		Syslog - 4 event types covering admin access and AAA authentication		Juniper Networks Steel-Belted Radius
Juniper	Secure Access Gateway	SNMP: OS, Hardware	SNMP: CPU, Memory, Disk, Interface utilization	Syslog - Over 30 event types parsed for situations covering VPN login, Admin access, Configuration Change		Juniper Networks SSL VPN Gateway
Juniper	Netscreen IDP			Syslog - directly from Firewall or via NSM -		Juniper Networks IDP Series

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				Over 5500 IPS Alert types parsed		
Juniper	DDoS Secure			Syslog - DDoS Alerts		Juniper DDoS
Lantronix	SLC Console Manager			Syslog - Admin access, Updates, Commands run		Lantronix SLC Console Manager
LastLine				Syslog in CEF format		LastLine
Liebert	HVAC	SNMP: Host Name, Hardware model	SNMP: HVAC metrics: Temperature: current value, upper threshold, lower threshold, Relative Humidity: current value, upper threshold, lower threshold, System state etc			Liebert HVAC
Liebert	FPC	SNMP: Host Name, Hardware model	SNMP: Output voltage (X-N, Y-N, Z-N), Output current (X, Y. Z), Neutral Current, Ground current, Output power, Power Factor etc			Liebert FPC
Liebert	UPS	SNMP: Host Name, Hardware model	SNMP: UPS metrics: Remaining battery charge, Battery status, Time on battery, Estimated Seconds Remaining, Output voltage etc			Liebert UPS
Malwarebytes	Malwarebytes Breach Remediation					Malwarebytes Breach Remediation
Malwarebytes	Malwarebytes Endpoint Protection					Malwarebytes Endpoint Protection
McAfee	Vormetric Data Security Manager	LOG Discovery	Currently not natively supported	1 broad event Type	Currently not natively supported	McAfee Vormetric Data Security Manager
Microsoft	ASP.NET	SNMP: Running Processes	SNMP or WMI: Process level resource usage ; WMI: Request Execution Time, Request Wait Time, Current Requests, Disconnected Requests etc			Microsoft ASP.NET
Microsoft	Microsoft Defender for Identity/Azure Advanced Threat	Host name and Device type	Not supported		Not supported	Microsoft Defender for Identity/Microsoft Azure ATP

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
	Protection (ATP)					
Microsoft	Azure Compute					Microsoft Azure Compute
Microsoft	Azure Event Hub					Microsoft Azure Event Hub
Microsoft	Cloud App Security	Host name and Device type	Not supported		Not supported	Microsoft Cloud App Security
Microsoft	DHCP Server - 2003, 2008	SNMP: Running Processes	WMI: DHCP metrics: request rate, release rate, decline rate, Duplicate Drop rate etc	FortiSIEM Windows Agent (HTTPS): DHCP logs - release, renew etc; Snare Agent (syslog): DHCP logs - release, renew etc; Correlog Agent (syslog): DHCP logs - release, renew etc		Microsoft DHCP (2003, 2008)
Microsoft	DNS Server - 2003, 2008	SNMP: Running Processes	WMI: DNS metrics: Requests received, Responses sent, WINS requests received, WINS responses sent, Recursive DNS queries received etc	FortiSIEM Windows Agent (HTTPS): DNS logs - name resolution activity; Snare Agent (syslog): DNS logs - name resolution activity; Correlog Agent (syslog): DNS logs - name resolution activity		Microsoft DNS (2003, 2008)
Microsoft	Domain Controller / Active Directory - 2003, 2008, 2012	SNMP: Running Processes; LDAP: Users	WMI: Active Directory metrics: Directory Search Rate, Read Rate, Write Rate, Browse Rate, LDAP search rate, LDAP Bind Rate etc; WMI: "dcdiag -e" command output - detect successful and failed domain controller diagnostic tests; WMI: "repadmin /replsummary" command output - Replication statistics; LDAP: Users with stale passwords, insecure password settings			Microsoft Active Directory
Microsoft	Exchange Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage; WMI: Exchange performance metrics, Exchange		Exchange Tracker Logs via FSM	Microsoft Exchange

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
			error metrics, Exchange mailbox metrics, Exchange SMTP metrics, Exchange ESE Database, Exchange Database Instances, Exchange Mail Submission Metrics, Exchange Store Interface Metrics etc		Advanced Windows Agent	
Microsoft	Hyper-V Hypervisor		Powershell over winexe: Guest/Host CPU usage, Memory usage, Page fault, Disk Latency, Network usage ;			Hyper-V
Microsoft	IIS versions	SNMP: Running Processes	SNMP or WMI: Process level resource usage WMI: IIS metrics: Current Connections, Max Connections, Sent Files, Received Files etc	FortiSIEM Windows Agent (HTTPS): W3C Access logs - Per instance Per Connection - Sent Bytes, Received Bytes, Duration ; Snare Agent (syslog): W3C Access logs; Correlog Agent (syslog): W3C Access logs		Microsoft IIS for Windows 2000 and 2003; Microsoft IIS for Windows 2008
Microsoft	Internet Authentication Server (IAS)	SNMP: Running Processes	SNMP or WMI: Process level resource usage	FortiSIEM Windows Agent (HTTPS): AAA logs - successful and failed authentication ; Snare Agent (syslog): AAA logs - successful and failed authentication ; Correlog Agent (syslog): AAA logs - successful and failed authentication		Microsoft Internet Authentication Server (IAS)
Microsoft	Network Policy Server	Discovered via LOG only.	Not natively supported. Custom monitoring needed.	AAA-based login events	Currently not natively supported	Microsoft Network Policy Server
Microsoft	PPTP VPN Gateway			FortiSIEM Windows Agent (HTTPS): VPN Access - successful and failed Snare Agent (syslog): VPN Access - successful and failed ; Correlog Agent (syslog): VPN Access -		Microsoft PPTP

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				successful and failed		
Microsoft	SharePoint Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage	LOGBinder Agent: SharePoint logs - Audit trail integrity, Access control changes, Document updates, List updates, Container object updates, Object changes, Object Import/Exports, Document views, Information Management Policy changes etc		Microsoft SharePoint
Microsoft	SQL Server - 2014, 2016, 2017, 2019	SNMP: Running Processes	SNMP or WMI: Process resource usage; JDBC: General database info, Configuration Info, Backup Info,; JDBC: Per-instance like Buffer cache hit ratio, Log cache hit ratio etc; JDBC: per-instance, per-database Performance metrics Data file size, Log file used, Log growths etc; JDBC: Locking info, Blocking info	JDBC: database error log; JDBC: Database audit trail		Microsoft SQL Server
Microsoft	Microsoft Defender for Endpoint/Windows Defender Advanced Threat Protection (ATP)	Host name and Device type	Not supported		Not supported	Microsoft Defender for Endpoint/Windows Defender ATP
Microsoft	Windows 2000, Windows 2003, Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2	SNMP: OS, Hardware (for Dell and HP), Installed Software, Running Processes; WMI: OS, Hardware (for Dell and HP), BIOS, Installed Software,	SNMP: CPU, Memory, Disk, Interface utilization, Process utilization ; WMI: SNMP: CPU, Memory, Disk, Interface utilization, Detailed CPU/Memory usage, Detailed Process utilization	WMI pulling: Security, System and Application logs; FortiSIEM Windows Agent (HTTPS): Security, System and Application logs, File Content change; Snare Agent (syslog): Security, System and Application logs; Correlog Agent (syslog): Security, System and Application	SNMP: Installed Software Change; FortiSIEM Windows Agent: Installed Software Change, Registry Change; FortiSIEM	Microsoft Windows Servers

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		Running Processes, Services, Installed Patches		logs	Windows Agent: File Integrity Monitoring	
MobileIron Sentry and Connector	Sentry	Discovered Via LOG only	Not natively supported - Custom monitoring needed	Over 18 Events Types parsed	Not natively supported - Custom configuration collection needed	MobileIron Sentry
Motorola	AirDefense Wireless IDS			Syslog: Wireless IDS logs		Motorola AirDefense
Motorola	WiNG WLAN Access Point			Syslog: All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health		Motorola WLAN
Mikrotek	Mikrotech Switches and Routers	Host name, OS, Hardware model, Serial number, Components	SNMP: Uptime CPU utilization, Network Interface metrics			Mikrotek Router
NetApp	DataONTAP					NetApp DataONTAP
NetApp	DataONTAP based Filers	SNMP: Host name, OS, Hardware model, Serial number, Network interfaces, Logical volumes, Physical Disks	SNMP: CPU utilization, Network Interface metrics, Logical Disk Volume utilization; SNMP: Hardware component health, Disk health ONTAP API: Detailed NFS V3/V4, ISCSI, FCP storage IO metrics, Detailed LUN metrics, Aggregate metrics, Volume metrics, Disk performance metrics	SNMP Trap: Over 150 alerts - hardware and software alerts		NetApp Filer
Nessus	Vulnerability Scanner			Nessus API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name,		Nessus Vulnerability Scanner

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence, etc		
Netwrix	Auditor	Not natively supported	Not natively supported	2 Event Types parsed (via Windows Correlog Agent)	Not natively supported	Netwrix Auditor
NGINX	Web Server	SNMP: Application name	SNMP: Application Resource Usage	Syslog: W3C access logs: per HTTP(S) connection: Sent Bytes, Received Bytes, Connection Duration		NGINX Web Server
Nimble	NimbleOS Storage	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	SNMP: Uptime, Network Interface metrics, **Storage Disk Utilization** SNMP: Storage Performance metrics: Read rate (IOPS), Sequential Read Rate (IOPS), Write rate (IOPS), Sequential Write Rate (IOPS), Read latency, etc			Nimble Storage
Nortel	ERS Switches and Routers	SNMP: Host name, OS, Hardware model, Serial number, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Hardware Status			Nortel ERS and Passport Switch
Nortel	Passport Switches and Routers	SNMP: Host name, OS, Hardware model, Serial number, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Hardware Status			Nortel ERS and Passport Switch
Nozomi	Guardian	No	No	Yes	No	Nozomi
Nutanix	Controller VM	SNMP: Host name, OS, Hardware	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Disk Status,			Nutanix

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		model, Serial number, Network interfaces, Physical Disks, Components	Cluster Status, Service Status, Storage Pool Info, Container Info			
Okta.com	SSO	Okta API: Users		Okta API: Over 90 event types covering user activity in Okta website		Okta Configuration
One Identity	Safeguard		Not supported			One Identity Safeguard
OpenLDAP	OpenLDAP	LDAP: Users				
Oracle	Cloud Access Security Broker (CASB)					Oracle Cloud Access Security Broker
Oracle	Enterprise Database Server - 10g, 11g, 12c	SNMP or WMI: Process resource usage ;	JDBC: Database performance metrics: Buffer cache hit ratio, Row cache hit ratio, Library cache hit ratio, Shared pool free ratio, Wait time ratio, Memory Sorts ratio etc ; JDBC: Database Table space information: able space name, table space type, table space usage, table space free space, table space next extent etc; JDBC: Database audit trail: Database logon, Database operations including CREATE/ALTER/DROP/TRUNCATE operations on tables, table spaces, databases, clusters, users, roles, views, table indices, triggers etc.	Syslog: Listener log, Alert log, Audit Log		Oracle Database
Oracle	MySQL Server	SNMP or WMI: Process resource usage	JDBC: User Connections, Table Updates, table Selects, Table Inserts, Table Deletes, Temp Table Creates, Slow Queries etc; JDBC: Table space performance metrics: Table space name, table space type, Character set and Collation, table space usage,			MySQL Server

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
			table space free space etc; JDBC: Database audit trail: Database log on, Database/Table CREATE/DELETE/MODIFY operations			
Oracle	WebLogic Application Server	SNMP or WMI: Process resource usage	JMX: Availability metrics, Memory metrics, Servlet metrics, Database metrics, Thread pool metrics, EJB metrics, Application level metrics			Oracle WebLogic
Oracle	Glassfish Application Server	SNMP or WMI: Process resource usage	JMX: Availability metrics, Memory metrics, Servlet metrics, Session metrics, Database metrics, Request processor metrics, Thread pool metrics, EJB metrics, Application level metrics, Connection metrics			Oracle GlassFish Server
Oracle	Sun SunOS and Solaris	SNMP: OS, Hardware, Software, Processes, Open Ports ; SSH: Hardware details	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification		Sun Solaris Server
PacketFence	Network Access Control	Host name and Device type	Not supported		Not supported	PacketFence Network Access Control
Palo Alto Networks	Palo Alto Traps Endpoint Security Manager	LOG Discovery	Currently not natively supported	Over 80 event types	Currently not natively supported	Palo Alto Traps Endpoint Security Manager
Palo Alto Networks	PAN-OS based Firewall	SNMP: Host name, OS, Hardware, Network interfaces; SSH: Configuration	SNMP: Uptime, CPU utilization, Network Interface metrics, Firewall connection count	Syslog: Traffic log, Threat log (URL, Virus, Spyware, Vulnerability, File, Scan, Flood and data subtypes), config and system logs	SSH: Configuration Change	Palo Alto Firewall
Proofpoint	Proofpoint					Proofpoint
PulseSecure	PulseSecure VPN			Syslog: VPN events, Traffic events, Admin events		PulseSecure

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
QNAP	Turbo NAS					QNAP Turbo NAS
Qualys	QualysGuard Scanner					Qualys QualysGuard Scanner
Qualys	Vulnerability Scanner			Qualys API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence etc		Qualys Vulnerability Scanner
Qualys	Web Application Firewall			syslog (JSON formatted): web log analysis		Qualys Web Application Firewall
Radware	DefensePro	LOG Discovery	Currently not natively supported	Over 120 event types	Currently not natively supported	Radware DefensePro
Rapid7	InsightVM (Platform Based Vulnerability Management)	Host name and Device type	Not supported			Rapid7 InsightVM (Vulnerability Management On-Premises)
Rapid7	NeXpose Vulnerability Scanner (Vulnerability Management On-Premises)			Rapid7 NeXpose API: Vulnerability Scan results - Scan name, Host, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulnerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence etc		Rapid7 NeXpose Vulnerability Scanner (Platform Based Vulnerability Management)
Riverbed	Steelhead WAN Accelerators	SNMP: Host name, Software version,	SNMP: Uptime, CPU / Memory / Network Interface / Disk space metrics, Process cpu/memory	SNMP Trap: About 115 event types covering software errors, hardware errors, admin		Riverbed SteelHead WAN Accelerator

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		Hardware model, Network interfaces	utilization; SNMP: Hardware Status SNMP: Bandwidth metrics: (Inbound/Outbound Optimized Bytes - LAN side, WAN side; Connection metrics: Optimized/Pass through / Half-open optimized connections etc); SNMP: Top Usage metrics: Top source, Top destination, Top Application, Top Talker; SNMP: Peer status: For every peer: State, Connection failures, Request timeouts, Max latency	login, performance issues - cpu, memory, peer latency issues ; Netflow: Connection statistics		
Redhat	Linux	SNMP: OS, Hardware, Software, Processes, Open Ports ; SSH: Hardware details, Linux distribution	SNMP: CPU, Memory, Disk, Interface utilization, Process monitoring, Process stop/start, Port up/down ; SSH: Disk I/O, Paging	Syslog: Situations covering Authentication Success/Failure, Privileged logons, User/Group Modification SSH: File integrity monitoring, Command output monitoring, Target file monitoring Agent: File integrity monitoring	SSH: File integrity monitoring, Target file monitoring Agent: File integrity monitoring	Linux Server
Redhat	JBOSS Application Server	SNMP: Process level CPU/Memory usage	JMX: CPU metrics, Memory metrics, Servlet metrics, Database pool metrics, Thread pool metrics, Application level metrics, EJB metrics	;		Redhat JBOSS
Redhat	DHCP Server	SNMP: Process level CPU/Memory usage		Syslog: DHCP address release/renew events		Linux DHCP
Ruckus	Wireless LAN	SNMP: Controller host name, Controller hardware model, Controller network interfaces, Associated	SNMP: Controller Uptime, Controller Network Interface metrics, Controller WLAN Statistics, Access Point Statistics, SSID performance Stats			Ruckus WLAN

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
		WLAN Access Points				
Security Onion	Zeek (Bro)	Discovered via LOG only	Not natively supported - Custom monitoring needed	Syslog JSON format: 6 event types parsed	Currently not natively supported	Zeek (Bro) Installed on Security Onion
SentinelOne	SentinelOne	Discovered via LOG only	Not natively supported. Custom monitoring needed.	System and security events (e.g. file blocked)	Currently not natively supported	SentinelOne
Snort	IPS	SNMP: Process level CPU/Memory usage		Syslog: Over 40K IPS Alerts DBC: Over 40K IPS Alerts - additional details including TCP/UDP/ICMP header and payload in the attack packet		Snort IPS
Sophos	Central	Host name and Device type	Not supported		Not supported	Sophos Central
Sophos	Sophos Endpoint Security and Control			SNMP Trap: Endpoint events including Malware found/deleted, DLP events		Sophos Endpoint Security and Control
Squid	Web Proxy	SNMP: Process level CPU/Memory usage		Syslog: W3C formatted access logs - per HTTP (S) connection: Sent Bytes, Received Bytes, Connection Duration		Squid Web Proxy
SSH Com Security	CryptoAuditor	LOG Discovery	Currently not natively supported	Many event types	Currently not natively supported	SSH Com Security CryptoAuditor
Stormshield	Network Security	Not natively supported	Not natively supported	Firewall logs	Not natively supported	Stormshield Network Security
Symantec	Symantec Endpoint Protection			Syslog: Over 5000 event types covering end point protection events - malware/spyware/adware, malicious events		Symantec Endpoint Protection
Tanium	Connect	Host name and Device type	Not supported		Not supported	Tanium Connect

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
Tenable	Tenable.io	Host name and Device type	Not supported		Not supported	Tenable.io
Tigera	Calico	Not natively supported	Not natively supported	Flow, Audit and DNS logs	Not natively supported	Tigera Calico
TrendMicro	Deep Discovery	Discovered via LOG only	Not natively supportedCustom monitoring needed.	Malicious file detection	Currently not natively supported	TrendMicro Deep Discovery
TrendMicro	Deep Security Manager			Syslog: Over 10 event types covering end point protection events	Not supported	
TrendMicro	Interscan Web Filter	LOG Discovery	Currently not natively supported	15 event Types	Currently not natively supported	TrendMicro Interscan Web Filter
TrendMicro	Intrusion Defense Firewall (IDF)			Syslog: Over 10 event types covering end point firewall events		Trend Micro IDF
TrendMicro	Office scan			SNMP Trap: Over 30 event types covering end point protection events - malware/spyware/adware, malicious events		Trend Micro OfficeScan
Vasco	DigiPass			Syslog - Successful and Failed Authentications, Successful and Failed administrative logons		Vasco DigiPass
VMware	VMware ESX and VCenter	VMWare SDK: Entire VMware hierarchy and dependencies - Data Center, Resource Pool, Cluster, ESX and VMs	VMWare SDK: VM level: CPU, Memory, Disk, Network, VMware tool status VMWare SDK: ESX level: CPU, Memory, Disk, Network, Data store VMWare SDK: ESX level: Hardware Status VMWare SDK: Cluster level: CPU, Memory, Data store, Cluster Status VMWare SDK: Resource pool level: CPU, Memory	VMWare SDK: Over 800 VCenter events covering account creation, VM creation, DRS events, hardware/software errors		
VMware	vShield			Syslog: Over 10 events covering permitted and denied connections,		

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Config Change Monitoring	Details
				detected attacks		
VMware	VCloud Network and Security (vCNS) Manager			Syslog: Over 10 events covering various activities		
WatchGuard	Firebox Firewall			Syslog: Over 20 firewall event types		WatchGuard Firebox Firewall
Websense	Web Filter			Syslog: Over 50 web filtering events and web traffic logs		Websense Web Filter
YXLink	Vulnerability Scanner					YX Link Vulnerability Scanner

Applications

This section describes how to configure applications for discovery and for providing information to FortiSIEM.

- Application Server
- Authentication Server
- Database Server
- DHCP and DNS Server
- Directory Server
- Document Management Server
- Healthcare IT
- Mail Server
- Management Server/Appliance
- Remote Desktop
- Source Code Control
- Unified Communication Server
- Web Server

Application Server

FortiSIEM supports the discovery and monitoring of these application servers.

- Apache Tomcat
- IBM WebSphere
- Microsoft ASP.NET
- Oracle GlassFish Server
- Oracle WebLogic
- Redhat JBOSS

Apache Tomcat

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Event for Tomcat Metrics

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		**Generic information:** Application version, Application port **Availability metrics:** Uptime, Application Server State **CPU metrics:** CPU utilization **Memory metrics:** Total memory, Free memory, Memory utilization, Virtual committed memory, Total Swap Memory, Free Swap Memory**,** Swap memory utilization, Heap Utilization, Heap Used Memory, Heap max memory, Heap commit memory, Non-heap Utilization, Non-heap used memory, Non-heap max memory, Non-heap commit memory **Servlet metrics:** Web application name, Servlet Name, Count allocated, Total requests, Request errors, Load time, Avg Request Processing time **Session metrics:** Web context path, Peak active sessions, Current active sessions, Duplicate sessions, Expired sessions, Rejected sessions, Average session lifetime, Peak session lifetime, Session processing time, Session create rate, Session expire rate, Process expire frequency, Max session limited, Max inactive Interval	Performance Monitoring
JMX		**Database metrics:** Web context path, Data source, Database driver, Peak active sessions, Current active sessions, Peak idle sessions, Current idle sessions **Thread pool metrics:** Thread pool name, Application port, Total threads, Busy threads, Keep alive threads, Max threads, Thread priority, Thread pool daemon flag **Request processor metrics:** Request processor name, Received Bytes, Sent Bytes, Average Request Process time, Max Request Processing time, Request Rate, Request Errors	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "tomcat" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "tomcat" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

JMX

Add the necessary parameters to the Tomcat startup script.

- Windows
- Linux

Windows

Modify the file `${CATALINA_BASE}\bin\catalina.bat` by adding these arguments for JVM before the comment:

```
rem ----Execute The Requested Command ------
```

JMX Configuration for Windows

```
set JAVA_OPTS=-Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.port=${Your
JMX Port} \ -Dcom.sun.management.jmxremote.authenticate=true \ -
Dcom.sun.management.jmxremote.ssl=false \ -
Dcom.sun.management.jmxremote.access.file=jmxremote.access \ -
Dcom.sun.management.jmxremote.password.file=jmxremote.password \
```

Linux

Modify the file ${CATALINA_BASE}/bin/catalina.sh by adding these arguments for JVM before the comment:

```
# ----Execute The Requested Command ------
```

JMX Configuration for Linux

```
JAVA_OPTS=" $ JAVA_OPTS -Dcom.sun.management.jmxremote \ -
Dcom.sun.management.jmxremote.port=${ Your JMX Port} \ -
Dcom.sun.management.jmxremote.authenticate=true \ -Dcom.sun.management.jmxremote.ssl=false
\ -Dcom.sun.management.jmxremote.access.file=jmxremote.access \ -
Dcom.sun.management.jmxremote.password.file=jmxremote.password" \
```

1. Edit the access authorization file `jmxremote.access`.

   ```
   monitorRole  readonly
   controlRole  readwrite
   ```

2. Edit the password file `jmxremote.password.`
   The first column is user name and the second column is password). FortiSIEM only needs monitor access.

   ```
   monitorRole  <FortiSIEMUserName>controlRole  <userName>
   ```

3. In Linux, set permissions for the jmxremote.access and jmxremote.password files so that they are read-only and accessible only by the Tomcat operating system user.

   ```
   chmod 600 jmxremote.access
   chmod 600 jmxremote.password
   ```

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Apache Tomcat application server over JMX:

Setting	Value
Name	Enter a name for the credential.
Device Type	Apache Apache Tomcat
Access Protocol	JMX
Pull Interval (minutes)	5
Port	0
User Name	The user you created in step 3
Password	The password you created in step 3

Sample Event for Tomcat Metrics

```
<134>Jan 22 01:57:32 10.1.2.16 java: [PH_DEV_MON_TOMCAT_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[appServerState]=STARTED,[sysUpTime]=2458304,[cpuUtil]=0

<134>Jan 22 01:57:32 10.1.2.16 java: [PH_DEV_MON_TOMCAT_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[appServerState]=STARTED,[freeMemKB]=116504,
[freeSwapMemKB]=2974020,[memTotalMB]=4095,[swapMemTotalMB]=8189,[virtMemCommitKB]=169900,
[memUtil]=98,[swapMemUtil]=65,[heapUsedKB]=18099,[heapMaxKB]=932096,[heapCommitKB]=48896,
[heapUtil]=37,[nonHeapUsedKB]=22320,[nonHeapMaxKB]=133120,[nonHeapCommitKB]=24512,
[nonHeapUtil]=91

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[webAppName]=//localhost/host-manager,
[servletName]=HTMLHostManager,[countAllocated]=0,[totalRequests]=0,[reqErrors]=0,
[loadTime]=0,[reqProcessTimeAvg]=0,[maxInstances]=20,[servletState]=STARTED
```

```
<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_SESSION]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[webContextPath]=/host-manager,[activeSessionsPeak]=0,
[activeSessions]=0,[duplicateSession]=0,[expiredSession]=0,[rejectedSession]=0,
[sessionLifetimeAvg]=0,[sessionLifetimePeak]=0,[sessionProcessTimeMs]=0,
[sessionCreateRate]=0,[sessionExpireRate]=0,[webAppState]=STARTED,
[processExpiresFrequency]=6,[maxSessionLimited]=-1,[maxInactiveInterval]=1800

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_DB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=9218,
[appVersion]=Apache Tomcat/7.0.27,[webContextPath]=/host-manager,
[dataSource]="jdbc/postgres1",[dbDriver]=org.postgresql.Driver,[activeSessionsPeak]=20,
[activeSessions]=0,[idleSessionsPeak]=10,[idleSessions]=0

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_THREAD_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
[destDevPort]=9218,[appVersion]=Apache Tomcat/7.0.27,[threadPoolName]=ajp-apr-18009,
[appPort]=18009,[totalThreads]=0,[busyThreads]=0,[keepAliveThreads]=0[maxThreads]=200,
[threadPriority]=5,[threadPoolIsDaemon]=true

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_REQUEST_PROCESSOR]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-
WIN08R2-JMX,[destDevPort]=9218,[appVersion]=Apache Tomcat/7.0.27,[reqProcessorName]="http-
apr-18080",[recvBytes]=0,[sentBytes]=62748914,[totalRequests]=4481,
[reqProcessTimeAvg]=44107,[reqProcessTimeMax]=516,[reqRate]=0,[reqErrors]=7
```

IBM WebSphere

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

HTTPS Preferred for Monitoring over JMX IBM WebSphere performance metrics can be obtained via HTTP(S) or JMX. The HTTP(S) based method is highly recommended since it consumes significantly less resources on FortiSIEM.

Protocol	Information discovered	Metrics collected	Used for
HTTP / HTTP(S)		**Generic information:** Application version, Application port **Availability metrics:** Uptime, Application Server State **CPU metrics:** Application server instance, CPU utilization **Memory metrics:** Heap utilization, Heap used memory, Heap free memory, Heap max memory, Heap commit memory **Servlet metrics:** Application name, Web application name, Servlet Name, Invocation count **Database pool metrics:** Application server instance, JDBC provider, Data source, Pool size, Closed connections, Active Connections, Requests wait for connections, Connection use time, Connection factory type, Peak connections **Thread pool metrics:** Application server instance, Thread pool name, Execute threads, Peak execute threads **Transaction metrics:** Application server instance, Active Transaction, Committed Transaction, Rolled back Transaction **Authentication metrics:** Application name, Application server instance, Authentication Method, Count	Performance Monitoring
JMX		**Generic information:** Application version, Application port **Availability metrics:** Uptime, Application Server State **CPU metrics:** Application server instance, CPU utilization **Memory metrics:** Heap utilization, Heap used memory, Heap free memory, Heap max memory, Heap commit memory, Max System dumps on disk, Max heap dumps on disk **Servlet metrics:** Application name, Web application name, Servlet Name, Invocation count, Request errors	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Database pool metrics: Application server instance, JDBC provider, Data source, Pool size, Closed connections, Active Connections, Requests wait for connections, Connection use time, Connection factory type, Peak connections **Thread pool metrics:** Application server instance, Thread pool name, Execute threads, Peak execute threads **Application level metrics:** Application name, Web application name, Application server instance, Web application context root, Active sessions, Peak active sessions **EJB metrics:** Application name, Application server instance, EJB component name	
Syslog			Log analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "websphere" to see the event types associated with this device.

- `PH_DEV_MON_WEBSPHERE_CPU (from HTTPS)`

  ```
  <134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_CPU]:[eventSeverity]=PHL_
  INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,
  [destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,[cpuUtil]=0,
  [sysUpTime]=2340206,[appServerState]=RUNNING
  ```

- `PH_DEV_MON_WEBSPHERE_CPU (from JMX)`

  ```
  <134>Jan 22 02:15:23 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_CPU]:[eventSeverity]=PHL_
  INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
  [destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
  [appServerInstance]=server1,[cpuUtil]=0,[sysUpTime]=42206,[appServerState]=STARTED
  ```

- `PH_DEV_MON_WEBSPHERE_MEMORY (from HTTPS)`

  ```
  <134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_MEMORY]:[eventSeverity]=PHL_
  INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,
  [destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,
  [appServerState]=running,[heapFreeKB]=93208,[heapUsedKB]=168936,[heapCommitKB]=232576,
  [heapMaxKB]=262144,[heapUtil]=72
  ```

- `PH_DEV_MON_WEBSPHERE_MEMORY (from JMX)`

  ```
  <134>Jan 22 02:15:25 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_MEMORY]:[eventSeverity]=PHL_
  INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
  [destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
  [appServerInstance]=server1,[appServerState]=STARTED,[maxSystemDumpsOnDisk]=10,
  [maxHeapDumpsOnDisk]=10,[heapFreeKB]=48140,[heapUsedKB]=172018,[heapCommitKB]=217815,
  [heapMaxKB]=262144,[heapUtil]=78
  ```

- `PH_DEV_MON_WEBSPHERE_APP (from HTTPS)`

```
 <134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_APP]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,
[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,[appName]=isclite,
[webAppName]=ISCAdminPortlet.war,[activeSessions]=0,[activeSessionsPeak]=1
```

- PH_DEV_MON_WEBSPHERE_APP (from JMX)

```
<134>Jan 22 02:18:24 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_APP]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
[destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
[appServerInstance]=server1,[appName]=isclite,[webAppName]=isclite.war,
[webContextRoot]=admin_host/ibm/console,[activeSessions]=0,[activeSessionsPeak]=1
```

- PH_DEV_MON_WEBSPHERE_SERVLET (from HTTPS)

```
 <134>Dec 08 16:11:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_SERVLET]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-
10.1.2.16,[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,
[appName]=isclite,[webAppName]=isclite.war,
[servletName]=/com.ibm.ws.console.servermanagement/collectionTableLayout.jsp,
[invocationCount]=2
```

- PH_DEV_MON_WEBSPHERE_SERVLET (from JMX)

```
 <134>Jan 22 02:15:24 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_SERVLET]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-
WIN08R2-JMX,[destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
[appServerInstance]=server1,[appName]=isclite,[webAppName]=isclite.war,
[servletName]=action,[reqErrors]=0,[invocationCount]=14
```

- PH_DEV_MON_WEBSPHERE_DB_POOL (from HTTPS)

```
<134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_DB_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-10.1.2.16,
[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,[jdbcProvider]=Derby
JDBC Provider (XA),[dataSource]=jdbc/DefaultEJBTimerDataSource,[poolSize]=0,
[closedConns]=0,[activeConns]=0,[waitForConnReqs]=0,[connUseTime]=0
```

- PH_DEV_MON_WEBSPHERE_DB_POOL (from JMX)

```
<134>Jan 22 02:15:23 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_DB_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
[destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
[appServerInstance]=server1,[jdbcProvider]=Derby JDBC Provider (XA),
[dataSource]=DefaultEJBTimerDataSource,[poolSize]=0,[closedConns]=0,[activeConns]=0,
[waitForConnReqs]=0,[connUseTime]=0,[connFactoryType]=,[peakConns]=0
```

- PH_DEV_MON_WEBSPHERE_THREAD_POOL (from HTTPS)

```
 <134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_THREAD_POOL]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-
10.1.2.16,[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,
[threadPoolName]=WebContainer,[executeThreads]=2,[executeThreadPeak]=6
```

- PH_DEV_MON_WEBSPHERE_THREAD_POOL (from JMX)

```
<134>Jan 22 02:18:25 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_THREAD_POOL]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-
WIN08R2-JMX,[destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
[appServerInstance]=server1,[threadPoolName]=ORB.thread.pool,[executeThreads]=0,
[executeThreadPeak]=0
```

- PH_DEV_MON_WEBSPHERE_TRANSACTION (from HTTPS)

```
<134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_TRANSACTION]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-
10.1.2.16,[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,
[activeTxCount]=0,[committedTxCount]=3406,[rolledBackTxCount]=0
```

- `PH_DEV_MON_WEBSPHERE_AUTHENTICATION (from HTTPS)`

```
 <134>Dec 08 16:14:55 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_AUTHENTICATION]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=Host-
10.1.2.16,[destDevPort]=9443,[appVersion]=8.5.5.3,[appServerInstance]=server1,
[authenMethod]=TokenAuthentication,[count]=0
```

- `PH_DEV_MON_WEBSPHERE_EJB (from JMX)`

```
<134>Jan 22 02:15:24 10.1.2.16 java: [PH_DEV_MON_WEBSPHERE_EJB]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
[destDevPort]=8880,[appVersion]=IBM WebSphere Application Server 7.0.0.11,
[appServerInstance]=server1,[appName]=SchedulerCalendars,
[ejbComponentName]=Calendars.jar
```

Reports

In **RESOURCES > Reports**, search for "websphere" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- HTTP(S)
  - Install the perfServletApp Application
  - Configure Security for the Application
  - Start the Application
- JMX
  - Configuring the Default JMX Port

HTTP(S)

Install the perfServletApp Application

1. Log in to your Websphere administration console.
2. Go to **Applications > Application Types > WebSphere enterprise application**.
3. Click **Install**.
4. Select **Remote file system** and browse to `{WebSphere_Home}/AppServer/installableApps/PerfServletApp.ear`.
5. Click **Next**.
   The **Context Root** for the application will be set to `/wasPerfTool`, but you can edit this during installation.

Configure Security for the Application

1. Go to **Security > Global Security**.
2. Select **Enable application security**.
3. Go to **Applications > Application Types > Websphere Enterprise Applications**.
4. Select **perfServletApp**.
5. Click **Security role to user/group mapping**.
6. Click **Map Users/Groups**.
7. Use the Search feature to find and select the FortiSIEM user you want to provide with access to the application,
8. Click **Map Special Subjects.**
9. Select **All Authenticated in Application's Realm**.
10. Click **OK**.

Start the Application

1. Go to **Applications > Application Types > WebSphere enterprise application**.
2. Select **perfServletApp**.
3. Click **Start**.
4. In a web browser, launch the application by going to `http://<ip>:<port>/wasPerfTool/servlet/perfservlet`. Default HTTP Port The default port for HTTP is 9080, HTTPS is 9443. You can change these by going to **Servers > Server Types > WebSphere application servers > {serverInstance} > Configuration > Ports**.

JMX

Configuring the Default JMX Port

By default, your Websphere application server uses port 8880 for JMX. You can change this by logging in to your application server console and going to **Application servers > {Server Name} > Ports > SOAP_CONNECTOR_ ADDRESS**. The username and password for JMX are the same as the credentials logging into the console. To configure JMX communications between your Websphere application server and FortiSIEM, you must copy several files from your application server to the Websphere configuration directory for each FortiSIEM virtual appliance that will be used for discovery and performance monitoring jobs. FortiSIEM does not include these files because of licensing restrictions.

1. Copy these files to the directory `/opt/phoenix/config/websphere/` for each Supervisor, Worker, and Collector in your FortiSIEM deployment.

File Type	Location
Client Jars	• `${WebSphere_Home}/AppServer/runtimes/com.ibm.ws.admin.client.jar` • `${WebSphere_Home}/AppServer/plugins/com.ibm.ws.security.crypto.jar`
SSL files	• `${WebSphere_Home}/AppServer/profiles/${Profile_Name}/etc/DummyClientKeyFile.jks` • `${WebSphere_Home}/AppServer/profiles/${Profile_Name}/etc/DummyClientTrustFile.jks`

2. Install IBM JDK 1.6 or higher in the location `/opt/phoenix/config/websphere/java` for each Supervisor, Worker, and Collector in your FortiSIEM deployment.

You can now configure FortiSIEM to communicate with your device by following the instructions in the *User Guide > Section: Setting Credentials*, and then initiate discovery of the device as described in the topics under *Discovery Settings*.

Settings for Access Credentials

Use these **Access Method Definition** options to let FortiSIEM access your IBM Websphere device over HTTPS and SNMP. When you set the **Device Credential Mapping Definition**, make sure to map both the HTTPS and SNMP credentials to the same IP address for your Websphere device.

- Settings for IBM Websphere HTTPS Access Credentials
- Settings for IBM Websphere SNMP Access Credentials
- SNMP Access Credentials for All Devices
- Settings for IBM Websphere JMX Access Credentials

Settings for IBM Websphere HTTPS Access Credentials

Setting	Value
Name	websphere_https
Device Type	IBM Websphere App Server
Access Protocol	HTTPS
Port	9443
URL	/wasPerfTools/servlet/perfservlet
User Name	Use the user name that you provided with access to the application
Password	The password associated with the user that has access to the application

Settings for IBM Websphere SNMP Access Credentials

Use these **Access Method Definition** settings to let FortiSIEM access your IBM Websphere device over SNMP. When you set the **Device Credential Mapping Definition**, make sure to map both the HTTPS and SNMP credentials to the same IP address for your Websphere device.

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Settings for IBM Websphere JMX Access Credentials

Use these **Access Method Definition** settings to let FortiSIEM access your IBM Websphere device over JMX.

Setting	Value
Name	websphere
Device Type	IBM Websphere App Server
Access Protocol	JMX
Pull Interval (minutes)	5
Port	8880
User Name	The administrative user for the application server
Password	The password associated with the administrative user

Microsoft ASP.NET

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Sample Event for ASP.NET Metrics

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
WMI		Request Execution Time, Request Wait Time, Current Requests, Disconnected Requests, Queued requests, Disconnected Requests	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "asp.net" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "asp.net" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

Sample Event for ASP.NET Metrics

```
[PH_DEV_MON_APP_ASPNET_MET]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=4868,[hostName]=QA-EXCHG,[hostIpAddr]=172.16.10.28,
[appGroupName]=Microsoft ASPNET,[aspReqExecTimeMs]=0,[aspReqCurrent]=0,
[aspReqDisconnected]=0,[aspReqQueued]=0,[aspReqRejected]=0,[aspReqWaitTimeMs]=0
```

Oracle GlassFish Server

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		**Generic information:** Application version, Application port **Availability metrics:** Uptime, Application Server State **CPU metrics:** CPU utilization **Memory metrics:** Total memory, Free memory, Memory utilization, Virtual committed memory, Total Swap Memory, Free Swap Memory, Swap memory utilization, Heap Utilization, Heap Used Memory, Heap max memory, Heap commit memory, Non-heap Utilization, Non-heap used memory, Non-heap max memory, Non-heap commit memory **Servlet metrics:** Web application name, Servlet Name, Count allocated, Total requests, Request errors, Avg Request Processing time	Performance Monitoring
JMX		**Session metrics:** Web context path, Peak active sessions, Current active sessions, Duplicate sessions, Expired sessions, Rejected sessions, Average session lifetime, Peak session lifetime, Session processing time, Session create rate, Session expire rate, Process expire frequency, Max session limited, Max inactive Interval **Database metrics:** Data source **Thread pool metrics:** Current live threads, Max live threads **Request processor metrics:** Request processor name, Received Bytes, Sent Bytes, Total requests, Average Request Process time, Max Request Processing time, Request Rate, Request Errors, Max open connections, Current open connections, Last Request URI, Last Request method, Last Request completion time	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Application level metrics: Cache TTL, Max cache size, Average request processing time, App server start time, Cookies allowed flag, Caching allowed flag, Linking allowed flag, Cross Context Allowed flag **EJB metrics**: EJB component name, EJB state, EJB start time **Connection metrics**: Request processor name, HTTP status code, HTTP total accesses	

Event Types

In **ADMIN > Device Support > Event Types**, search for "glassfish" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "glassfish" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

JMX

1. The default JMX port used by Oracle GlassFish is 8686. If you want to change it, modify the node `jmx-connector` of the file `${GlassFish_Home}\domains\${Domain_Name}\config\domain.xml`.
2. The username and password for JMX are the same as the web console.

You can now configure FortiSIEM to communicate with your device by following the instructions in "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Oracle GlassFish JMX Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Oracle GlassFish device over JMX.

Setting	Value
Name	glassfish
Device Type	SUN Glassfish App Server
Access Protocol	JMX
Pull Interval (minutes)	5

Setting	Value
Port	8686
User Name	The administrative user for the application server
Password	The password associated with the administrative user

Sample Event for Glassfish Metrics

```
<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,[webContextRoot]=,
[webAppState]=RUNNING,[cacheMaxSize]=10240,[cacheTTL]=5000,[reqProcessTimeAvg]=0,
[startTime]=1358755971,[cookiesAllowed]=true,[cachingAllowed]=false,[linkingAllowed]=false,
[crossContextAllowed]=true

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,[sysUpTime]=35266,
[cpuUtil]=60

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_MEMORY]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[freeMemKB]=479928,[freeSwapMemKB]=6289280,[memTotalMB]=16051,[memUtil]=98,[swapMemUtil]=1,
[swapMemTotalMB]=6142,[virtMemCommitKB]=4025864,[heapUsedKB]=1182575,[heapMaxKB]=3106432,
[heapCommitKB]=3106432,[heapUtil]=38,[nonHeapUsedKB]=193676,[nonHeapMaxKB]=311296,
[nonHeapCommitKB]=277120,[nonHeapUtil]=69

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_SESSION]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[webContextPath]=/__JWSappclients,[activeSessionsPeak]=0,[duplicateSession]=0,
[activeSessions]=0,[expiredSession]=0,[rejectedSession]=0,[sessionProcessTimeMs]=85,
[sessionLifetimeAvg]=0,[sessionLifetimePeak]=0,[maxSessionLimited]=-1,
[maxInactiveInterval]=1800

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_SERVLET]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[webAppName]=phoenix,[webAppState]=RUNNING,[servletName]=DtExportServlet,[totalRequests]=0,
[reqErrors]=0,[reqProcessTimeAvg]=0

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_CONN_STAT]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[reqProcessorName]=http8181,[httpStatusCode]=304,[httpTotalAccesses]=0

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_EJB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[ejbComponentName]=phoenix-domain-1.0.jar,[ejbState]=RUNNING,[startTime]=1358755963,

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_JMS]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[jmsSource]=jms/RequestQueue

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_REQUEST_PROCESSOR]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-
10.1.2.201,[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[reqProcessorName]=http4848,[recvBytes]=0,[sentBytes]=0,[totalRequests]=0,[reqRate]=0,
[reqProcessTimeAvg]=0,[reqProcessTimeMax]=0,[maxOpenConnections]=0,[lastRequestURI]=null,
[lastRequestMethod]=null,[lastRequestCompletionTime]=0,[openConnectionsCount]=0,
[reqErrors]=0

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_THREAD_POOL]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-
10.1.2.201,[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[liveThreads]=106,[liveThreadsMax]=138

<134>Jan 22 02:06:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_DB_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.201,[hostIpAddr]=10.1.2.201,[hostName]=Host-10.1.2.201,
[destDevPort]=8686,[appVersion]=Sun Java System Application Server 9.1_02,
[dataSource]=jdbc/phoenixDS
```

Oracle WebLogic

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Event for WebLogic Metrics

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		**Generic information:** Application version, Application port, SSL listen port, Listen port enabled flag, SSL listen port enabled **Availability metrics:** Uptime, Application Server State **Memory metrics:** Total memory, Free memory, Used memory, Memory utilization, Heap utilization, Heap used memory, Heap max memory, Heap commit memory, Total nursery memory **Servlet metrics:** Application name, App server instance, Web application name, Web context name, Servlet name, Invocation count, Servlet execution time **Database pool metrics:** Application name, App server instance, Data source, Active connection count, Connection limit, Leaked connections, Reserve requests, Requests wait for connections **Thread pool metrics:** App server instance, Completed requests, Execute threads, Pending requests, Standby threads, Total threads **EJB metrics:** EJB component name, EJB state, EJB idle beans, EJB used beans, EJB pooled beans, EJB Waiter threads, EJB committed Transactions, EJB timedout transactions, EJB rolledback transactions, EJB activations, EJB Passivations, EJB cache hits, EJB cache misses, EJB cache accesses, EJB cache hit ratio **Application level metrics:** Application name, App server instance, Web application name, Web context root, Peak active sessions, Current active sessions, Total active sessions, Servlet count, Single threaded servlet pool count,	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "WebLogic" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "WebLogic" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

JMX

Enable and Configure Internet Inter-ORB Protocol (IIOP)

1. Log into the administration console of your WebLogic application server.
2. In the **Change Center** of the administration console, click **Lock & Edit**.
3. In the left-hand navigation, expand **Environment** and select **Servers**.
4. Click the **Protocols** tab, then select **IIOP**.
5. Select **Enable IIOP**.
6. Expand the **Advanced** options.
7. For **Default IIOP Username and Default IIOP Password**, enter the username and password that you will use as the access credentials when configuring FortiSIEM to communicate with your application server.

Enable IIOP Configuration Changes

1. Go to the **Change Center** of the administration console.
2. Click **Activate Changes**.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Oracle WebLogic application server over JMX.

The port for JMX is the same as the web console, and the default value is 7001.

Setting	Value
Name	weblogic
Device Type	Oracle WebLogic App Server
Access Protocol	JMX
Pull Interval (minutes)	5
Port	7001

Setting	Value
User Name	The administrative user you created in step 7.
Password	The password you created in step 7.

Sample Event for WebLogic Metrics

```
<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_GEN]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appServerState]=RUNNING,[sysUpTime]=1358476145,
[appPort]=7001,[sslListenPort]=7002,[listenPortEnabled]=true,[sslListenPortEnabled]=true

<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appServerState]=RUNNING,[heapUsedKB]=153128,
[heapCommitKB]=262144,[heapFreeKB]=109015,[heapUtil]=59,[heapMaxKB]=524288,
[usedMemKB]=4086224,[freeMemKB]=107624,[memTotalMB]=4095,[memUtil]=97,[nurserySizeKB]=88324

<134>Jan 22 02:12:22 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appName]=consoleapp,[webAppName]=examplesServer_
/console,[servletName]=/framework/skeletons/wlsconsole/placeholder.jsp,
[webContextRoot]=/console,[invocationCount]=1094,[servletExecutionTimeMs]=63

<134>Jan 22 02:15:24 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_DB_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appName]=examples-demoXA-2,[dataSource]=examples-demoXA-
2,[activeConns]=0,[connLimit]=1,[leakedConns]=0,[reserveRequests]=0,[waitForConnReqs]=0

<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_THREAD_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
[destDevPort]=7001,[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[completedRequests]=14066312,[executeThreads]=7,
[pendingRequests]=0,[standbyThreads]=5,[totalThreads]=43

<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_EJB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[ejbComponentName]=ejb30,[ejbIdleBeans]=0,
[ejbUsedBeans]=0,[ejbPooledBeans]=0,[ejbWaiter]=0,[ejbCommitTransactions]=0,
[ejbTimedOutTransactions]=0,[ejbRolledBackTransactions]=0,[ejbActivations]=0,
[ejbPassivations]=0,[ejbCacheHits]=0,[ejbCacheMisses]=0,[ejbCacheAccesses]=0,
[ejbCacheHitRatio]=0

<134>Jan 22 02:12:23 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=7001,
[appVersion]=WebLogic Server 10.3  Fri Jul 25 16:30:05 EDT 2008 1137967 ,
[appServerInstance]=examplesServer,[appName]=webservicesJwsSimpleEar,
[webAppName]=examplesServer_/jws_basic_simple,[webContextRoot]=/jws_basic_simple,
[activeSessions]=0,[activeSessionsPeak]=0,[activeSessionTotal]=0,[numServlet]=4,
[singleThreadedServletPool]=5
```

Redhat JBOSS

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Event for JBOSS Metrics

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
JMX		**Generic information:** Application version, Application port **Availability metrics:** Uptime, Application Server State **CPU metrics:** Application server instance, CPU utilization **Memory metrics:** Heap utilization, Heap used memory, Heap free memory, Heap max memory, Heap commit memory, Max System dumps on disk, Max heap dumps on disk **Servlet metrics:** Application name, Web application name, Servlet Name, Invocation count, Request errors **Database pool metrics:** Application server instance, JDBC provider, Data source, Pool size, Closed connections, Active Connections, Requests wait for connections, Connection use time, Connection factory type, Peak connections **Thread pool metrics:** Application server instance, Thread pool name, Execute threads, Peak execute threads **Application level metrics:** Application name, Web application name, Application server instance, Web application context root, Active sessions, Peak active sessions **EJB metrics:** Application name, Application server instance, EJB component name	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "jboss" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "jboss" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- Configuring JMX on the JBOSS Application Server
- Configuring FortiSIEM to Use the JMX Protocol with JBOSS Application Server

Configuring JMX on the JBOSS Application Server

Changing the Default JMX Port

The default port for JMX is 1090. If you want to change it, modify the file `${JBoss_Home}\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml.`

```
<bean class="org.boss.services.bindging.ServiceBindingMetadata">   <property
name="serviceName">jboss.remoting:service=JMXConnectorServer,protocol=rmi</property>
<property name="port">1090</property>   <property name="description">RMI/JRMP socket for
connecting to the JMX MBeanServer</property></bean>
```

1. Enable authentication security check. Open the file `${JBoss_Home}\server\default\deploy\jmx-jboss-beans.xml`, find the `JMXConnector` bean, and uncomment the `securityDomain` property.

   ```
   <bean name="JMXConnector" class="org.boss.system.server.jmx.JMXConnector"><!--
   configuration properties -->
   <!-- To enable authentication security checks, uncomment the following --!><!--UNCOMMENT
   THIS --><property name="securityDomain">jmx-console</property>
   ```

2. Modify the file `${JBoss_Home}\server\default\conf\props\jmx-console-roles.properties` to configure the JMX administrator role.

   ```
   admin=JBossAdmin,HttpInvoker
   ```

3. Modify the file `${JBoss_Home}\server\default\conf\props\jmx-console-users.properties` to configure the username and password for JMX.

   ```
   admin=yourpassword
   ```

4. Configure DNS resolution for the JBOSS application server in your FortiSIEM Supervsior, Workers, and Collectors by adding the IP address and DNS name of the JBOSS application server to their `/etc/hosts` files. If DNS is already configured to resolve the JBOSS application server name, you can skip this step.
5. Start JBoss.

   ```
   ${JBoss_Home}/bin/run.sh   -b  0.0.0.0
   or
   ${JBoss_Home}/bin/run.sh   -b  ${Binding IP}
   ```

Configuring FortiSIEM to Use the JMX Protocol with JBOSS Application Server

To configure JMX communications between your JBOSS application server and FortiSIEM, you must copy several files from your application server to the JBOSS configuration directory for each FortiSIEM virtual appliance that will be used for discovery and performance monitoring jobs. FortiSIEM does not include these files because of licensing restrictions.

JBOSS Version	Files to Copy
4.x, 5.x, 6.x	Copy `${JBoss_Home}/lib/jboss-bootstrap-api.jar` to `/opt/phoenix/config/JBoss/`
7.0	No copying is necessary
7.1	Copy `${JBoss_Home}/bin/client/jboss-client.jar` to `/opt/phoenix/config/JBoss/`

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Redhat JBOSS device over JMX:

Setting	Value
Name	jboss
Device Type	Redhat JBOSS App Server
Access Protocol	JMX
Pull Interval (minutes)	5
Port	8880
User Name	The user you created in step 2
Password	The password you created for the user in step 3

Sample Event for JBOSS Metrics

```
<134>Feb 06 11:38:35 10.1.2.16 java: [PH_DEV_MON_JBOSS_CPU]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[appServerState]=STARTED,[sysUpTime]=6202359,[cpuUtil]=2
```

```
<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_MEMORY]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[appServerState]=STARTED,[freeMemKB]=264776,
[freeSwapMemKB]=1427864,[memTotalMB]=4095,[memUtil]=94,[swapMemUtil]=83,
[swapMemTotalMB]=8189,[virtMemCommitKB]=1167176,[heapUsedKB]=188629,[heapMaxKB]=466048,
[heapCommitKB]=283840,[heapUtil]=66,[nonHeapUsedKB]=106751,[nonHeapMaxKB]=311296,
[nonHeapCommitKB]=107264,[nonHeapUtil]=99
```

```
<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_APP]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[webContextRoot]=//localhost/,[webAppState]=RUNNING,
[cacheMaxSize]=10240,[cacheTTL]=5000,[reqProcessTimeAvg]=10472,[startTime]=1353919592,
[cookiesAllowed]=true,[cachingAllowed]=true,[linkingAllowed]=false,
[crossContextAllowed]=true
```

```
<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_SERVLET]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[webAppName]=//localhost/admin-console,[servletName]=Faces
Servlet,[totalRequests]=6,[reqErrors]=0,[loadTime]=0,[reqProcessTimeAvg]=10610

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_DB_POOL]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[dataSource]=DefaultDS,[dataSourceState]=Started


<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_REQUEST_PROCESSOR]:
[eventSeverity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-
WIN08R2-JMX,[destDevPort]=1090,[appVersion]=6.1.0.Final "Neo",[reqProcessorName]=ajp-
0.0.0.0-8009,[recvBytes]=0,[sentBytes]=0,[reqProcessTimeAvg]=0,[reqProcessTimeMax]=0,
[totalRequests]=0,[reqRate]=0,[reqErrors]=0

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_EJB]:[eventSeverity]=PHL_INFO,
[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,[destDevPort]=1090,
[appVersion]=6.1.0.Final "Neo",[ejbComponentName]=ejbjar.jar,
[ejbBeanName]=HelloWorldBeanRemote,[ejbAvailCount]=0,[ejbCreateCount]=0,[ejbCurrCount]=0,
[ejbMaxCount]=0,[ejbRemovedCount]=0,[ejbInstanceCacheCount]=null,[ejbPassivations]=null,
[ejbTotalInstanceCount]=null

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_THREAD_POOL]:[eventSeverity]=PHL_
INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-JMX,
[destDevPort]=1090,[appVersion]=6.1.0.Final "Neo",[threadPoolName]=ajp-0.0.0.0-8009,
[appPort]=8009,[totalThreads]=0,[busyThreads]=0,[maxThreads]=2048,[threadPriority]=5,
[pollerSize]=32768,[threadPoolIsDaemon]=true
```

Authentication Server

FortiSIEM supports these authentication servers for discovery and monitoring.

- Cisco Access Control Server (ACS)
- Cisco Duo
- Cisco Identity Solution Engine (ISE)
- CyberArk Password Vault
- Fortinet FortiAuthenticator
- Juniper Networks Steel-Belted Radius
- Microsoft Internet Authentication Server (IAS)
- Microsoft Network Policy Server (RAS VPN)
- One Identity Safeguard
- Vasco DigiPass

Cisco Access Control Server (ACS)

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O	Performance Monitoring
Syslog	Application type	Successful and Failed Authentications, Successful and Failed administrative logons, RADIUS accounting logs	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco secure acs" to see the event types associated with this device.

Configuration

- SNMP
- WMI
- Syslog

SNMP

1. Log into the device you want to enable SNMP for as an administrator.
2. Go to **Control Panel >Program and Features**.
3. Click **Turn Windows features on or off**.
4. If you are installing on a Windows 7 device, select **Simple Network Management Protocol (SNMP)**.
   If you are installing on a Windows 2008 device, in the **Server Manager** window, go to **Features > Add features > SNMP Services**.
5. If necessary, select SNMP to enable the service.
6. Go to **Programs > Administrative Tools > Services**.
7. to set the SNMP community string and include FortiSIEM in the list of hosts that can access this server via SNMP.
8. Select **SNMP Service** and right-click **Properties**.

9. Set the community string to **public**.
10. Go to the **Security** tab and enter the FortiSIEM IP Address.
11. Restart the SNMP service.

WMI

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- Creating a Generic User Who Does Not Belong to the Local Administrator Group
- Creating a User Who Belongs to the Domain Administrator Group

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add.**
6. Find the user you created, and then click **OK**.
   This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions,** click **EditDefault**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.

13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Enable remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Pane > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user for the @accelops.com domain.
   For example, **YJTEST@accelops.com**.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2.**
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced.**
8. Select the user you created for the monitoring account, and then click **Edit.**
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services.**
13. Select **Windows Management Instrumentation**, and then click **Restart.**

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and the click **OK**.

Syslog

1. Log in to your Cisco Access Controls Server as an administrator.
2. Go to **Start > All Programs > CiscoSecure ACS v4.1 > ACS Admin**.
3. In the left-hand navigation, click System Configuration, then click **Logging**.

4. Select **Syslog** for **Failed Attempts**, **Passed Authentication**, and **RADIUS Accounting** to send these reports to FortiSIEM.
5. For each of these reports, click **Configure** under **CSV**, and select the following attributes to include in the CSV output.

Report	CSV Attributes
Failed Attempts	• Message-Type • User-Name • NAS-IP-Address • Authen-Failure-Code • Author-Failure-Code • Caller-ID • NAS-Port • Author-Date • Group-Name • Filter Information • Access Device • AAA Server
Passed Authentication	• Message-Type • User-Name • NAS-IP-Address • Authen-Failure-Code • Author-Failure-Code • Caller-ID • NAS-Port • Author-Date • Group-Name • Filter Information • Access Device • AAA Server • Proxy-IP-Address • Source-NAS • PEAP/EAP-FAST-Clear-Name • Real Name
RADIUS Accounting	• User-Name • NAS-IP-Address • NAS-Port • Group-Name • Service-Type • Framed-Protocol • Framed-IP-Address • Calling-Station-Id • Acct-Status-Type • Acct-Input-Octets • Acct-Output-Octets

Report	CSV Attributes
	• Acct-Session-Id • Acct-Session-Time • Acct-Input-Packets • Acct-Output-Packets

6. For each of these reports, click **Configure** under **Syslog**, and for **Syslog Server**, enter the **IP** address of the FortiSIEM virtual appliance that will receive the syslog as the syslog server, enter 514 for **Port**, and set **Max message length** to **1024**.
7. To make sure your changes take effect, go to **System Configuration > Service Control**, and click **Restart ACS**.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Cisco Identity Solution Engine (ISE)

- Integration Points
- Event Types
- Configuration
- Access Credentials

Integration Points

Protocol	Information Discovered	Used For
Syslog	AAA log - authentication	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "Cisco-ISE" in the main content panel **Search...** field to see the event types associated with this device.

Configuration

- Configuring Cisco ISE
- Configuring FortiSIEM

Configuring Cisco ISE

Follow Cisco ISE documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes Cisco ISE syslog as long it follows the following format as shown in the sample syslog:

```
<181>Sep 21 06:50:51 fcmb-hq-psn01 CISE_Passed_Authentications 0000066354 3 0 2016-09-
21 06:50:51.516 +01:00 2915312533 5200 NOTICE Passed-Authentication: Authentication
succeeded, ConfigVersionId=287, Device IP Address=1.1.1.1,
DestinationIPAddress=1.1.1.2, DestinationPort=1812, UserName=00-15-65-20-33-E5,
Protocol=Radius, RequestLatency=33, NetworkDeviceName=ACME, User-Name=johndoe, NAS-IP-
Address=1.1.1.2, NAS-Port=50009, Service-Type=Call Check, Framed-IP-Address=1.1.1.2,
Framed-MTU=1500, Called-Station-ID=38-1C-1A-87-87-09, Calling-Station-ID=00-15-65-20-
33-E5, NAS-Port-Type=Ethernet, NAS-Port-Id=FastEthernet0/9, EAP-Key-Name=, cisco-av-
pair=service-type=Call Check, cisco-av-pair=audit-session-id=AC1B35F8000001240FC38F8A,
OriginalUserName=0015652033e5, AcsSessionID=fcmb-hq-psn01/251903157/22970712,
AuthenticationIdentityStore=Internal Endpoints, AuthenticationMethod=Lookup,
SelectedAccessService=Default Network Access, SelectedAuthorizationProfiles=IP_Phones,
```

Access Credentials

For Device Type Cisco Identity Solutions Engine, see Access Credentials.

Cisco Duo

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOGs Collected	Used For
API	Host name and Device Type from LOG, Login Audit Trail	4 log types	Security and Compliance

Event Types

Go to **Admin > Device Type > Event Types** and search for “Cisco-Duo”.

Rules

None

Reports

None

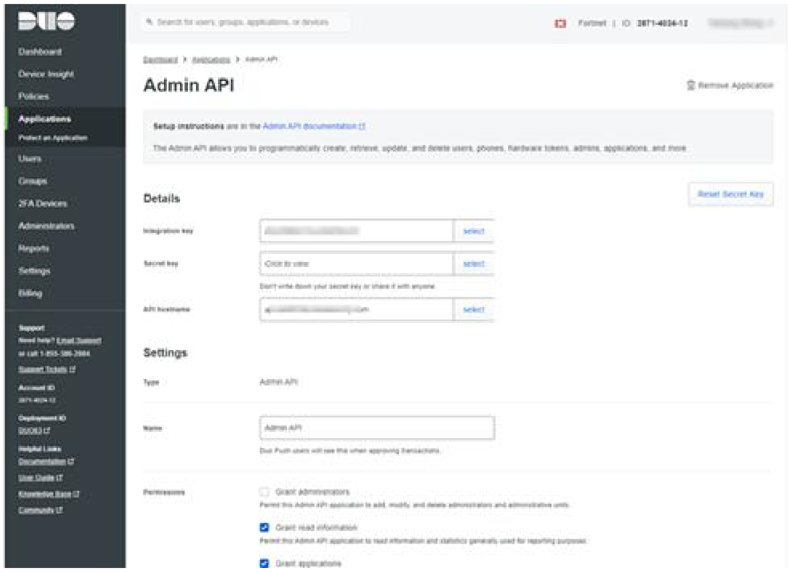
Configuration

- Configuring Cisco Duo
- Configuring FortiSIEM

Configuring Cisco Duo

Follow these steps to configure Cisco Duo to send logs to FortiSIEM.

1. Contact Cisco Duo support to enable the Admin API.
2. Get a credential for Cisco Duo: open the Cisco Duo dashboard and go to **Application > Admin API**.
3. Select the **Integration key**, **Secret key**, and **API hostname** options.



Admin API

Setup instructions are in the Admin API documentation

The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.

Details

Integration key

Secret key: Click to view

Don't write down your secret key or share it with anyone.

API hostname

Settings

Type: Admin API

Name: Admin API

Duo Push users will see this when approving transactions.

Permissions

□ Grant administrators

Permit this Admin API application to add, modify, and delete administrators and administrative units.

☑ Grant read information

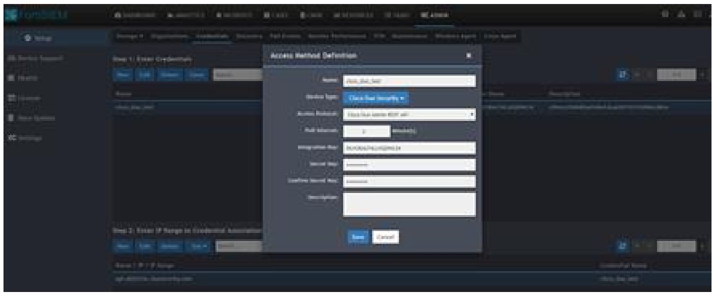
Permit this Admin API application to read information and statistics generally used for reporting purposes.

☑ Grant applications

Configuring FortiSIEM

Follow these steps to configure FortiSIEM to receive Cisco Duo logs.

1. In the FortiSIEM UI, go to **ADMIN > Setup > Credentials**.
2. In **Step 1: Enter Credentials**, click **New** to create a Cisco Duo credential.

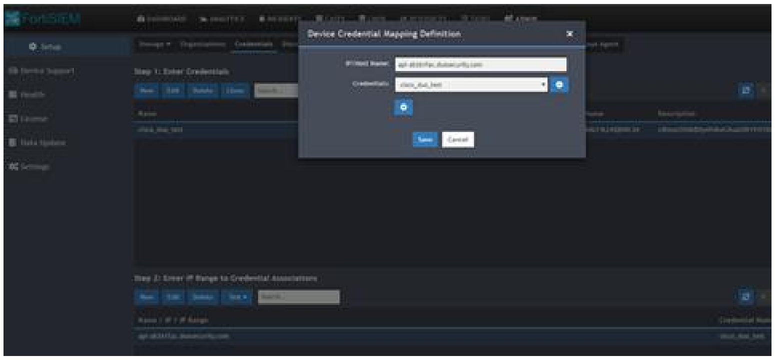


Use these Access Method Definition settings to allow FortiSIEM to access Cisco Duo logs.

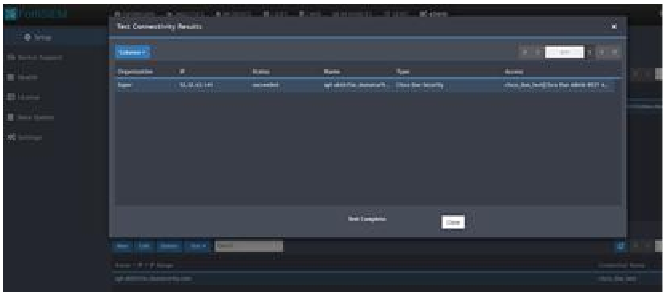
Setting	Value
Name	Enter a name for the credential.
Device Type	Cisco Duo Security
Access Protocol	Cisco Duo Admin REST API
Pull Interval (minutes)	2
Integration Key	Enter the integration key you obtained from Cisco Duo.
Secret Key	Enter the secret key you obtained from Cisco Duo.

Setting	Value
Description	Enter an optional description for the credential.

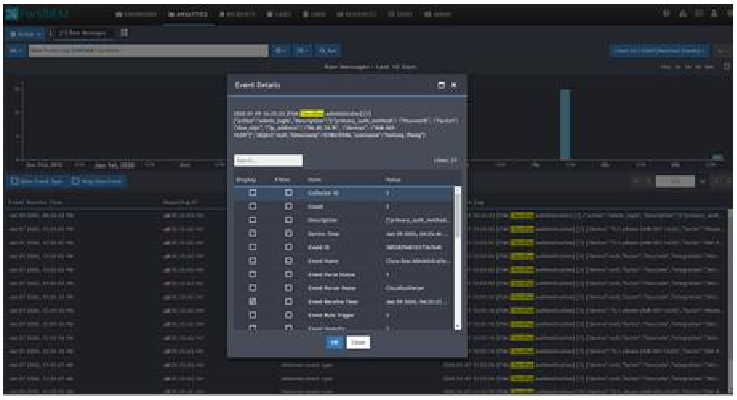
3. In **Step 2: Enter IP Range to Credentials Associations**, click **New** to create a new association between the credential and the API hostname.


FortiSIEM
Device Credential Mapping Definition
Save
Cancel
Step 1: Enter Credentials
Step 2: Enter IP Range to Credential Associations

4. Click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the connectivity results.



5. Go to the **ANALYTICS** page and check for Cisco Duo logs.



Sample Events

These events are collected via API:

```
FSM-CiscoDuo-Auth] [1] {"access_device":{"browser":"Chrome","browser_
version":"67.0.3396.99","flash_
version":"uninstalled","hostname":"null","ip":"169.232.89.219","java_
version":"uninstalled","location":{"city":"Ann Arbor","country":"United
States","state":"Michigan"},"os":"Mac OS X","os_version":"10.14.1"},"application":
{"key":"DIY231J8BR23QK4UKBY8","name":"Microsoft Azure Active Directory"},"auth_device":
{"ip":"192.168.225.254","location":{"city":"Ann Arbor","country":"United
States","state":"Michigan"},"name":"My iPhone X (734-555-2342)"},"event_
type":"authentication","factor":"duo_push","reason":"user_
approved","result":"success","timestamp":1532951962,"trusted_endpoint_status":"not
trusted","txid":"340a23e3-23f3-23c1-87dc-1491a23dfdbb","user":
{"key":"DU3KC77WJ06Y5HIV7XKQ","name":"narroway@example.com"}}
```

CyberArk Password Vault

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.0

Supported Versions:

- CyberArk Version 12.2 and earlier

Vendor: CyberArk

Product Information: https://www.cyberark.com/

Using CyberArk as a Credential Vault with FortiSIEM

The CyberArk Vault can be utilized by FortiSIEM to securely access and retrieve usernames and passwords for authentication against devices and applications. To use this feature, both CyberArk and FortiSIEM must be configured.

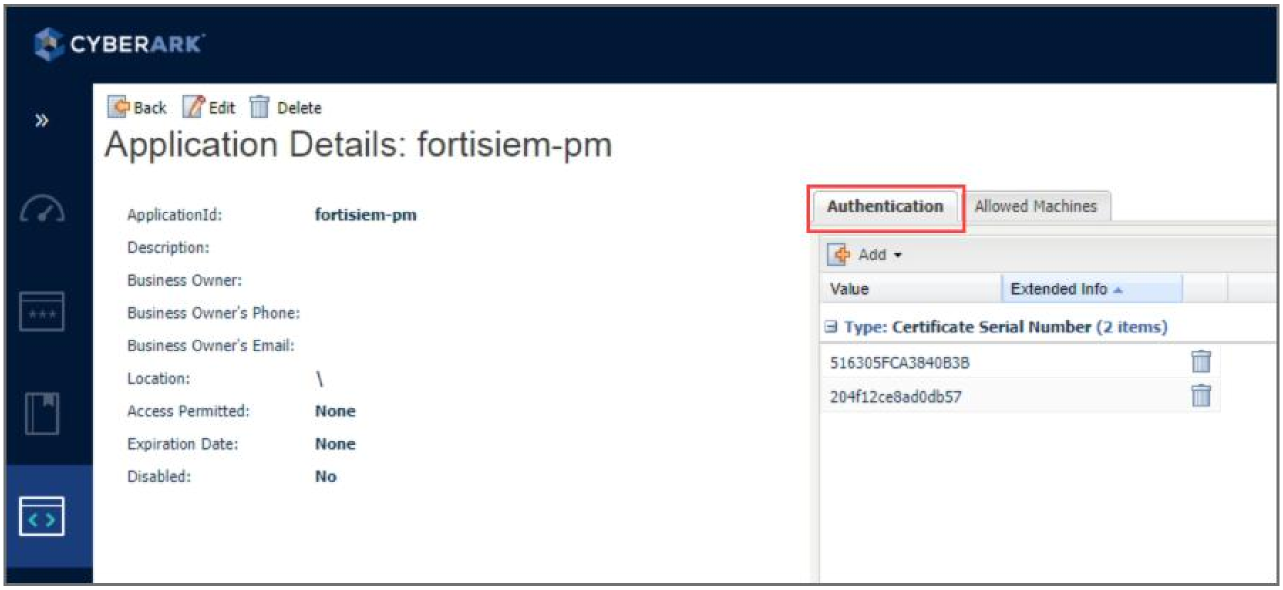
Configuring CyberArk

There are two methods to integrate CyberArk with FortiSIEM, using the REST API (CCP) or Java SDK. FortiSIEM supports both methods, however the preferred method is the REST API. The following steps provide instructions for configuration through the REST API.

After logging into CyberArk, take the following steps:

1. Go to the **Applications** section.
2. Create a new application and in the **Name** field, enter a name.
   or
   Select an existing application.

3. Select the **Authentication** tab.

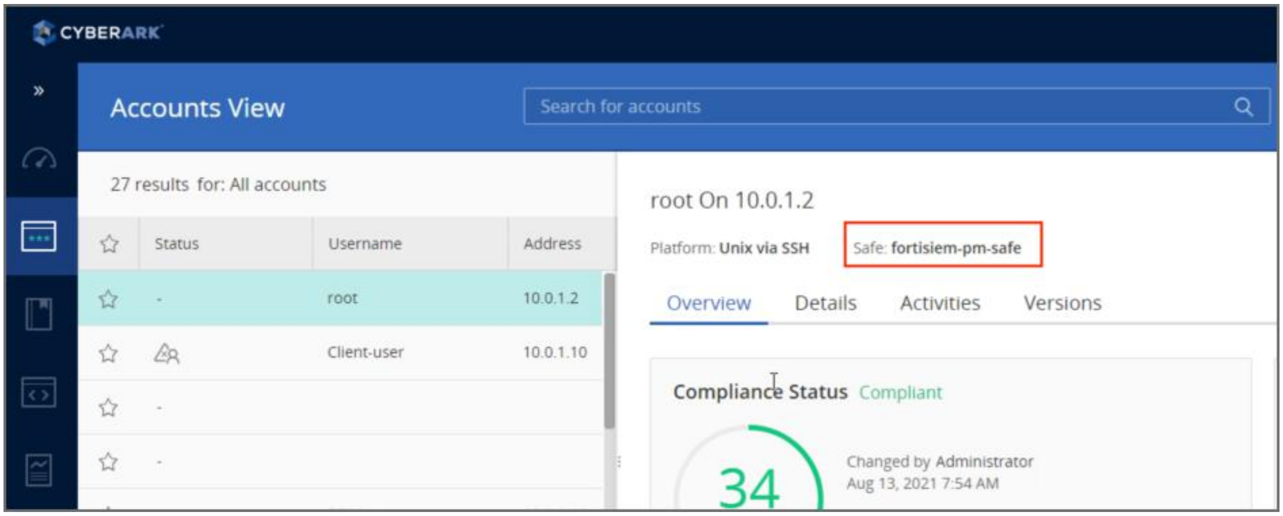


Application Details: fortisiem-pm

ApplicationId: fortisiem-pm
Description:
Business Owner:
Business Owner's Phone:
Business Owner's Email:
Location: \
Access Permitted: None
Expiration Date: None
Disabled: No

Value	Extended Info
Type: Certificate Serial Number (2 items)	
516305FCA3840B3B	
204f12ce8ad0db57	

4. Create certificates, and download the following:
Note: FortiSIEM requires the use of certificates as part of the authentication.
   - Root CA
   - SSL Certificate
   - SSL Key File
5. Ensure that the application has access to the Safe where the Credentials are stored.



27 results for: All accounts

Status	Username	Address
-	root	10.0.1.2
	Client-user	10.0.1.10
-		
-		

root On 10.0.1.2

Platform: Unix via SSH Safe: fortisiem-pm-safe

Compliance Status Compliant

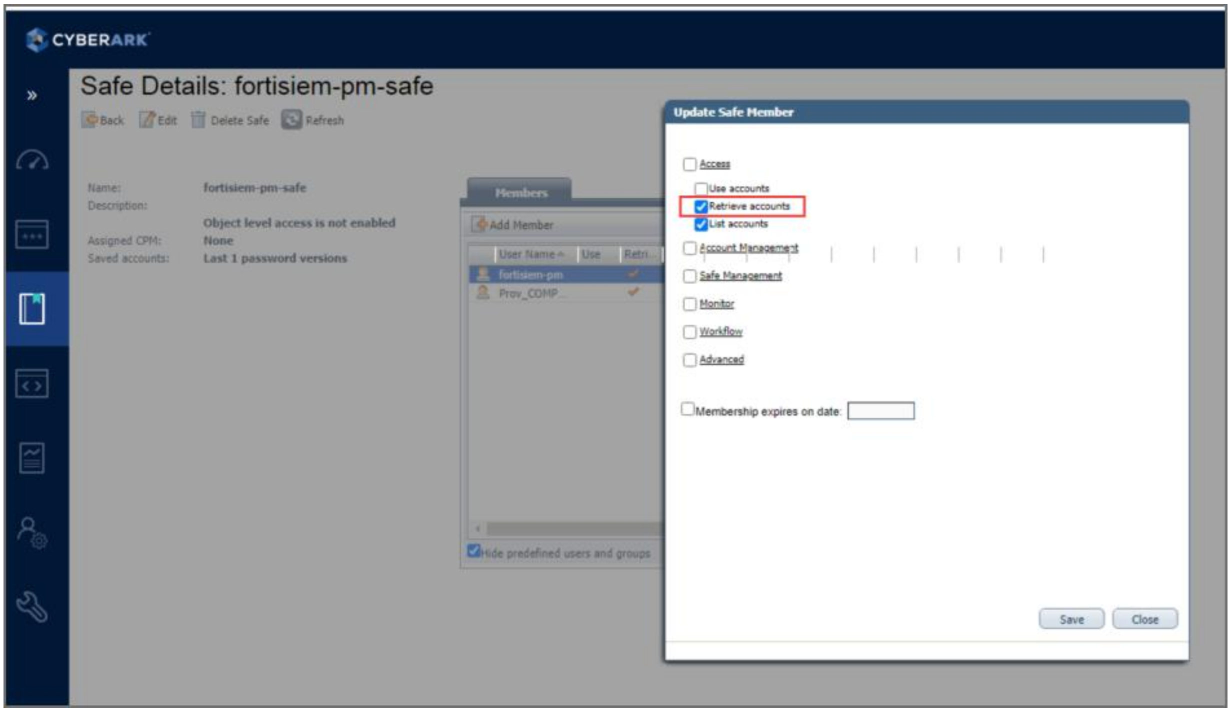
34

Changed by Administrator
Aug 13, 2021 7:54 AM

If you need to associate the Credential with a Safe, take the following steps:

a. Navigate to **Policy**.
b. Locate the Safe.
c. Click **Members**.
d. Click **Add Member**.
e. Add the Application.

f. Ensure the **Retrieve accounts** checkbox is checked. If it isn't, enable it.



Name: fortisiem-pm-safe
Description:
Object level access is not enabled
Assigned CPM: None
Saved accounts: Last 1 password versions

☑ Hide predefined users and groups

- ☐ Access
  - ☐ Use accounts
  - ☑ Retrieve accounts
  - ☑ List accounts
- ☐ Account Management
- ☐ Safe Management
- ☐ Monitor
- ☐ Workflow
- ☐ Advanced

☐ Membership expires on date:

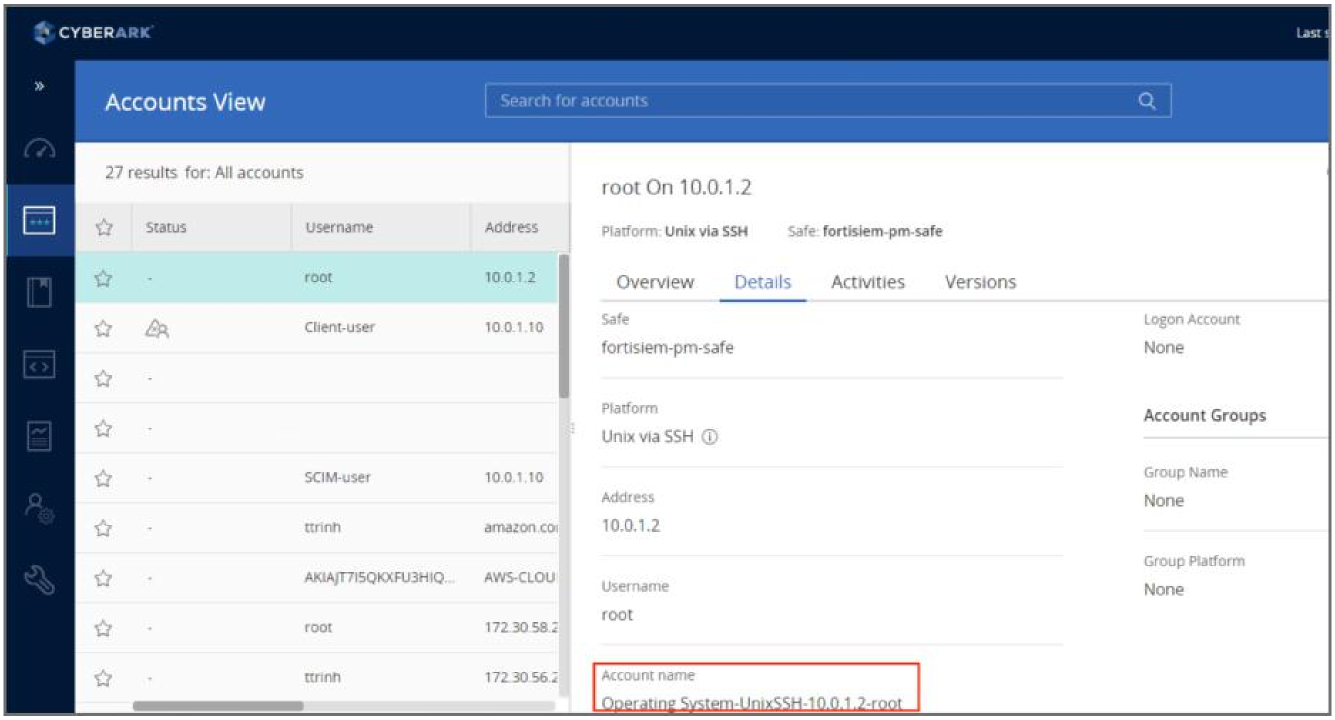
Configuring FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Navigate to **ADMIN > Setup** and click the **Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Setting	Value
Name	Enter the name of the credential.
Device Type	Define the device type.
Access Protocol	Define the access protocol.
Password Config	Select **CyberArk Rest API**.
Endpoint	Enter the DNS name or IP of the CyberArk server. The format should be https://<*server*>:<*port*>
Root CA	Upload the Root CA from CyberArk.
SSL Certificate	Upload the SSL Certificate from CyberArk.
SSL Key File	Upload the SSL Key File from CyberArk.
App ID	Provide the application defined in

Setting	Value
	CyberArk.
Safe	Provide the safe defined in CyberArk.
Folder	Provide the folder from the CyberArk configuration. If folders are not used, specify "root".
Object	Provide the credential Account Name from CyberArk. This can be found in CyberArk under **Accounts > *<your account>* > Details > *<Account Name>***. **Note**: See screenshot below for example Account Name. If the Object is defined in the FortiSIEM credential, then the follow additional details should not be needed: • Username • Platform (Policy ID) • Database • (Checkbox) Include Address for Query If this information is required, it can be obtained by using the thick client CyberArk tool PrivateArk. Take the following steps: **1.** Open PrivateArk. **2.** Open the Vault. **3.** Find the Safe you wish to use. **4.** Locate the credential, right click and select **Properties**. Here you will find the Username and Policy ID.



27 results for: All accounts

Status	Username	Address
-	root	10.0.1.2
	Client-user	10.0.1.10
-		
-		
-	SCIM-user	10.0.1.10
-	ttrinh	amazon.coı
-	AKIAJT7I5QKXFU3HIQ...	AWS-CLOU
-	root	172.30.58.2
-	ttrinh	172.30.56.2

root On 10.0.1.2

Platform: **Unix via SSH** Safe: **fortisiem-pm-safe**

Safe
fortisiem-pm-safe

Platform
Unix via SSH ⓘ

Address
10.0.1.2

Username
root

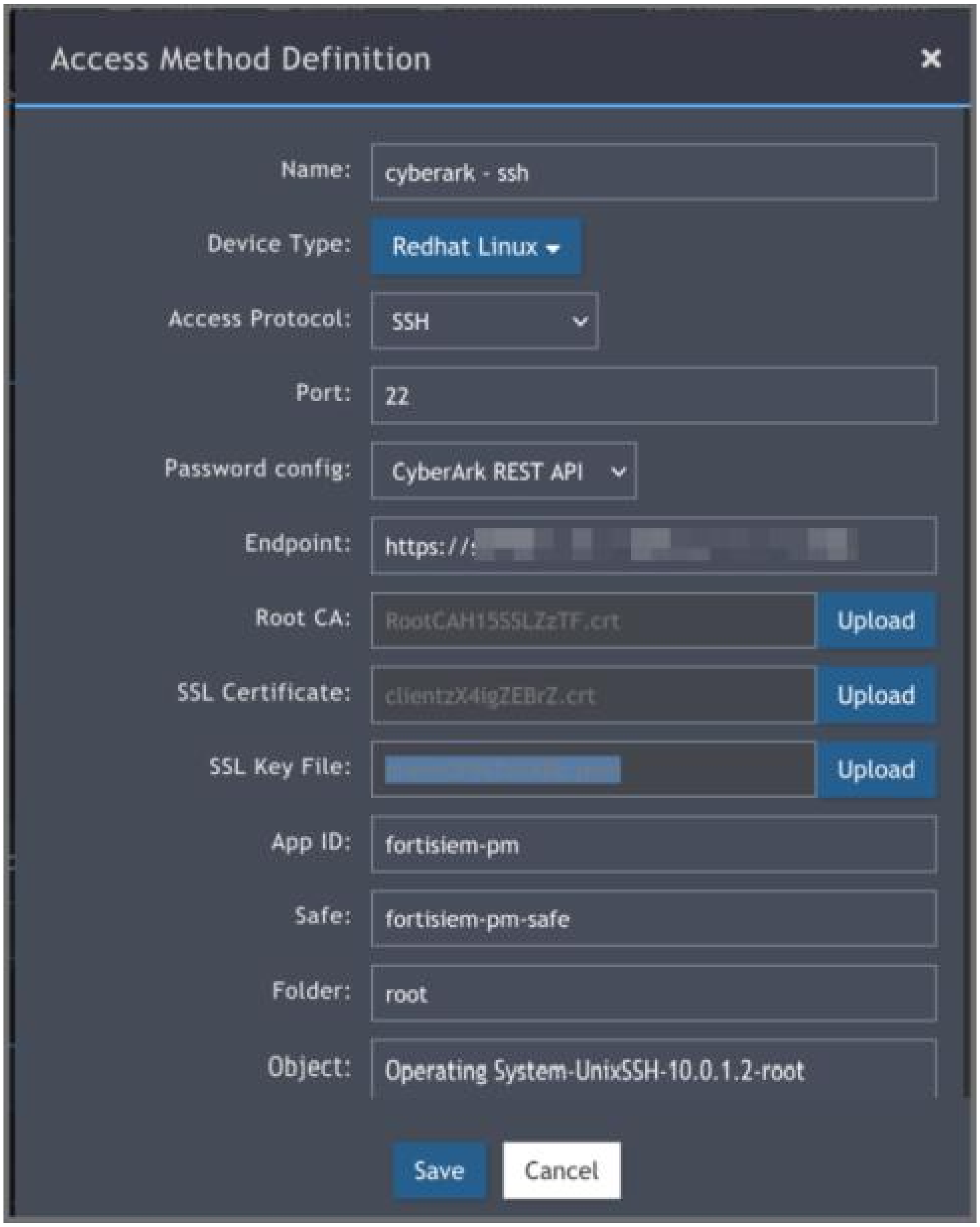
Account name
Operating System-UnixSSH-10.0.1.2-root

Logon Account
None

Account Groups

Group Name
None

Group Platform
None



Name: cyberark - ssh

Device Type: Redhat Linux

Access Protocol: SSH

Port: 22

Password config: CyberArk REST API

Endpoint: https://[redacted]

Root CA: RootCAH15SSLZzTF.crt

SSL Certificate: clientzX4igZEBrZ.crt

SSL Key File: [redacted]

App ID: fortisiem-pm

Safe: fortisiem-pm-safe

Folder: root

Object: Operating System-UnixSSH-10.0.1.2-root

What is Discovered and Monitored

Protocol	Information discovered	Logs parsed	Used for
Syslog (CEF formatted and others)		CyberArk Safe Activity	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "CyberArk-Vault" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "CyberArk" in the in the main content panel **Search...** field:

- CyberArk Vault Blocked Failure
- CyberArk Vault CPM Password Disables
- CyberArk Vault Excessive Failed PSM Connections
- CyberArk Vault Excessive Impersonations
- CyberArk Vault Excessive PSM Keystroke Logging Failure
- CyberArk Vault Excessive PSM Session Monitoring Failure
- CyberArk Vault Excessive Password Release Failure
- CyberArk Vault File Operation Failure
- CyberArk Vault Object Content Validation Failure
- CyberArk Vault Unauthorized User Stations
- CyberArk Vault User History Clear

Reports

In **RESOURCES > Reports**, search for "CyberArk" in the main content panel **Search...** field:

- CyberArk Blocked Operations
- CyberArk CPM Password Disables
- CyberArk CPM Password Retrieval
- CyberArk File Operation Failures
- CyberArk Impersonations
- CyberArk Object Content Validation Failures
- CyberArk PSM Monitoring Failures
- CyberArk Password Resets
- CyberArk Privileged Command Operations
- CyberArk Provider Password Retrieval
- CyberArk Trusted Network Area Updates
- CyberArk Unauthorized Stations
- CyberArk User History Clears
- CyberArk User/Group Modification Activity
- CyberArk Vault CPM Password Reconcilations
- CyberArk Vault CPM Password Verifications
- CyberArk Vault Configuration Changes
- CyberArk Vault Failed PSM connections
- CyberArk Vault Modification Activity
- CyberArk Vault PSM Keystore Logging Failures

- CyberArk Vault Password Changes from CPM
- CyberArk Vault Password Release Failures
- CyberArk Vault Successful PSM Connections
- Top CyberArk Event Types
- Top CyberArk Safes, Folders By Activity
- Top CyberArk Users By Activity

CyberArk Configuration for Sending syslog in a Specific Format

1. Open \PrivateArk\Server\DBParm.ini file and edit the SYSLOG section:
   a. SyslogServerIP – Specify FortiSIEM supervisor, workers and collectors separated by commas.
   b. SyslogServerProtocol – Set to the default value of UDP.
   c. SyslogServerPort – Set to the default value of 514.
   d. SyslogMessageCodeFilter – Set to the default range 0-999.
   e. SyslogTranslatorFile – Set to Syslog\FortiSIEM.xsl.
   f. UseLegacySyslogFormat - Set to the default value of No.
2. Copy the relevant XSL translator file here to the Syslog subfolder specified in the SyslogTranslatorFile parameter in DBParm.ini.
3. Stop and Start Vault (Central Server Administration) for the changes to take effect.

Make sure the syslog format is as follows.

```
<5>1 2016-02-02T17:24:42Z SJCDVVWCARK01 CYBERARK:
Product="Vault";Version="9.20.0000";MessageID="295";Message="Retrieve
password";Issuer="Administrator";Station="10.10.110.11";File="Root\snmpCommunity";
Safe="TestPasswords";Reason="Test";Severity="Info"
<30>Mar 22 20:13:42 VA461_1022 CyberArk AIM[2453]: APPAP097I Connection to the Vault has
been restored
<27>Mar 22 20:10:50 VA461_1022 CyberArk AIM[2453]: APPAP289E Connection to the Vault has
failed. Further attempts to connect to the Vault will be avoided for [1] minutes.
<27>Mar 24 23:41:58 VA461_1022 CyberArk AIM[2453]: APPAU002E Provider [Prov_VA461_1022] has
failed to fetch password with query [Safe=TestPutta;Object=Telnet91] for application
[FortiSIEM]. Fetch reason: [APPAP004E Password object matching query
```

Fortinet FortiAuthenticator

- What is Discovered and Monitored
- Event Types
- Configuration
- FortiSIEM Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
SNMP	Vendor, OS, Model, Network Interfaces	Interface Stat, Authentication Stat	Performance Monitoring
Syslog	LOG Discovery	Over 150 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "FortiAuthenticator" in the main content panel **Search...** field.

Sample Event Type:

```
<14>Aug 14 22:32:52 db[16987]:  category="Event" subcategory="Authentication" typeid=20995
level="information" user="admin" nas="" action="Logout" status="" Administrator 'admin'
logged out
```

Configuration

FortiAuthenticator logging instructions can be found here: https://docs.fortinet.com/document/fortiauthenticator/6.3.1/administration-guide/964220/log-configuration

Configure FortiAuthenticator to send logs to FortiSIEM by taking the following steps:

Create a Syslog Server

1. From FortiAuthenticator, navigate to **Logging > Log Config > Syslog Servers**.
2. Click **Create New**.
3. In the **Name** field, enter a name such as "FortiSIEM Collector".
4. In the **Server name/IP** field, enter the FortiSIEM Collector IP address.
5. In the **Port** field, ensure 514 is configured.
6. Click **OK** to add the syslog server.

Configure Remote Logging

1. Navigate to **Logging > Log Config > Log Settings**.
2. Go to **Remote Syslog** and make sure **Send system logs to remote Syslog servers** is enabled.

3. Move the "FortiSIEM Collector" syslog server to which logs will be sent from the **Available Syslog Servers** box to the **Chosen Syslog Servers** box.
4. Select **OK** to save your settings.

FortiSIEM Access Credentials

For **Device Type**, select Fortinet FortiAuthenticator from the drop-down list. See Access Credentials for more information on configuration.

Juniper Networks Steel-Belted Radius

- What is Discovered and Monitored
- Event Types
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O	Performance Monitoring
Syslog	Application type	Successful and Failed Authentications, Successful and Failed administrative logons, RADIUS accounting logs	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Juniper-Steelbelt" to see the event types associated with this device.

Configuration

- SNMP
- Syslog

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

1. Login as administrator.
2. Install and configure Epilog application to convert log files written by Steel-belted Radius server into syslog for sending to FortiSIEM:
   a. Download Epilog from snare, information to download here, and install it on your Windows Server.
   b. Launch Epilog from Start→All Programs→InterSect Alliance→Epilog for windows.

c. Configure Epilog application as follows:
   i. Select Log Configuration on left hand panel, click Add button to add log files whose content must be sent to FortiSIEM. These log files are written by the Steelbelted RADIUS server and their paths are correct. Also make sure the Log Type is SteelbeltedLog.
   ii. Select Network Configuration on left hand panel. On the right, set the destination address to that of FortiSIEM server, port to 514 and make sure that syslog header is enabled. Then click Change Configuration button.
   iii. Click the "Apply the latest audit configuration" link on the left hand side to apply the changes to Epilog applications. DHCP logs will now sent to FortiSIEM in real time.

Microsoft Internet Authentication Server (IAS)

- What is Discovered and Monitored
- Event Types
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
WMI			
Syslog			
Windows Agent			IAS logs

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft isa" to see the event types associated with this device.

Configuration

- WMI
- Syslog

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

Syslog

You must configure your Microsoft Internet Authentication Server to save logs, and then you can use the Windows Agent Manager to configure the type of log information you want sent to FortiSIEM.

1. Log in to your server as an administrator.
2. Go to **Start > Administrative Tools > Internet Authentication Service**.
3. In the left-hand navigation, select Remote Access Logging, then select **Local File**.
4. Right-click on **Local File** to open the **Properties** menu, and then select **Log File**.
5. For **Directory**, enter `C:\WINDOWS\system32\LogFiles\IAS`.
6. Click **OK**.

You can now use Windows Agent Installation Guide to configure what information will be sent to FortiSIEM.

Microsoft Network Policy Server (RAS VPN)

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Setting for Access Credentials
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	AAA based login events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "MS-NPS" to see the event types associated with this device.

Rules

No specific rules are written for Microsoft Network Policy Server, but regular AA Server rules apply.

Reports

No specific reports are written for Microsoft Network Policy Server, but regular AA Server reports apply.

Configuration

Configure Microsoft Network Policy Server system to send logs to FortiSIEM in the supported format (see Sample Events). See https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-accounting-configure.

Settings for Access Credentials

None required.

Sample Events

```
"HOSTXXVPN","RAS",03/10/2019,03:47:04,4,"domain\user",,"10.1.1.130","192.168.22.2",,"172.17.
     220.130",
"HOSTXXVPN","10.5.5.212",387,,"10.5.5.212","HOSTXXVPN",1552214822,,5,,1,2,,,0,
"311 1 fe80::a1bf:5c1c:7ebc:6ab7 02/07/2019 04:24:00
     4805",,,,,2,,268050551,253119217,"4806",3,69101,833955,726102,1,"1251",1,,79617,1,
"192.168.22.2","10.1.1.130",,,,,,,"MSRASV5.20",311,,"0x00504F4C42",0,,
"Microsoft Routing and Remote Access Service Policy",,,,"MSRAS-0-HOST123413","MSRASV5.20"
```

One Identity Safeguard (previously Balabit Privileged Session Management)

- Integration Points
- Event Types
- Configuration

Integration Points

Protocol	Information Discovered	Used For
Syslog	Privileged session management events	Security and Compliance

Event Types

Over 50 events are parsed. In **RESOURCES > Event Types**, search for "OneIdentity-Safeguard-" in the main content panel **Search...** field.

Configuration

- Configuring One Identity Safeguard
- Configuring FortiSIEM

Configuring One Identity Safeguard

Follow the One Identity Safeguard documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes One Identity Safeguard syslog as long as it follows the following format in the sample syslog:

```
<123>2018-10-08T22:59:49+08:00 scbdemo.balabit zorp/scb_rdp[31769]: core.debug(4):
(svc/i9CTbTzV2wrRur3quVRzF4/GET_gateway_rdp:498:2): After NAT mapping; nat_type='0',
src_addr='AF_INET(10.19.9.245:0)', dst_addr='AF_INET(10.46.26.196:3389)', new_addr='AF_
INET(10.11.101.30:0)'
```

Vasco DigiPass

- What is Discovered and Monitored
- Event Types
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		Successful and Failed Authentications, Successful and Failed administrative logons	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Vasco-DigiPass" to see the event types associated with this device. Some important ones are:

- Vasco-DigiPass-KeyServer-AdminLogon-Success
- Vasco-DigiPass-KeyServer-UserAuth-Success
- Vasco-DigiPass-KeyServer-UserAuth-Failed
- Vasco-DigiPass-KeyServer-AccountLocked
- Vasco-DigiPass-KeyServer-AccountUnlocked

Configuration

Configure the Vasco DigiPass management Console to send syslog to FortiSIEM. FortiSIEM is going to parse the logs automatically. Make sure the syslog format is as follows.

```
May 16 18:21:50 vascoservername ikeyserver[3575]: {Success}, {Administration}, {S-001003},
{A command of type [User] [Unlock] was successful.}, {0xA46B6230BA60B240CE48011B0C30D393},
{Source Location:10.1.2.3}, {Client Location:10.1.2.3}, {User ID:flast},
{Domain:company.com}, {Input Details: {User ID : flast} {Domain Name : company.com}},
{Output Details: {User ID : flast} {Password : ********} {Created Time : 2013/05/13
19:06:52} {Modified Time : 2013/05/16 18:21:49} {Has Digipass : Unassigned} {Status : 0}
{Domain Name : company.com} {Local Authentication : Default} {Back-end Authentication :
Default} {Disabled : no} {Lock Count : 0} {Locked : no} {Last Password Set Time : 2013/05/13
19:06:52} {Static Password History : d0NdVMhSdvdNEQJkkKTWmiq8iB4K1dWreMf5FQlZM7U=} {Key ID :
SSMINSTALLSENSITIVEKEY}}, {Object:User}, {Command:Unlock}, {Client Type:Administration
Program}

May 15 20:27:35 vascoservername ikeyserver[3575]: {Success}, {Administration}, {S-004001},
{An administrative logon was successful.}, {0x25AB20F3222F554A96CFFD2886AE4C71}, {Source
Location:10.1.2.3}, {Client Location:10.1.2.3}, {User ID:admin}, {Domain:company.com},
{Client Type:Administration Program}
```

```
May 17 18:43:22 vascoservername ikeyserver[3582]: {Info}, {Initialization}, {I-002010}, {The
SOAP protocol handler has been initialized successfully.},
{0x0E736D24D54E717E6F5DA6C09E89F8EE}, {Version:3.4.7.115}, {Configuration Details:IP-
Address: 10.1.2.3, IP-Port: 8888, Supported-Cipher-Suite: HIGH, Server-Certificate:
/var/identikey/conf/certs/soap-custom.pem, Private-Key-Password: ********, CA-Certificate-
Store: /var/identikey/conf/certs/soap-ca-certificate-store.pem, Client-Authentication-
Method: none, Reverify-Client-On-Reconnect: False, DPX-Upload-Location: /var/dpx/}
```

Database Server

FortiSIEM supports these database servers for discovery and monitoring.

- IBM DB2 Server
- Microsoft SQL Server
- MySQL Server
- Oracle Database Server

IBM DB2 Server

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials
- Sample Events

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
JDBC	None	**Database audit trail:** Successful and failed database log on, Database CREATE/DELETE/MODIFY operations, Table CREATE/DELETE/MODIFY/INSERT operations	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "db2" to see the event types associated with this device.

Configuration

- Configuring IBM DB2 Audit on Linux - DB2 side
- Configuring IBM DB2 Audit on Windows - DB2 side

Configuring IBM DB2 Audit on Linux - DB2 side

1. Log in to IBM Installation Manager.
2. Click the **Databases** tab, and click the **+** icon to create a new **Database Connection**.
3. Enter these settings.

Setting	Value
Database Connection Name	Enter a name for the connection, such as FortiSIEM
Data Server	DB2 for Linux, Unix, and Windows

Setting	Value
Type	
Database Name	Name of the database
Host name	db2.org
Port number	50000
JDBC Security	Clear text password
User ID	The username you want to use to access this Server from FortiSIEM
JDBC URL	jdbc:db2://db2.org:50000/<databasename>: retrieveMessagesFromServerOnGetMessage=true;securi

4. In the **Job Manager** tab, click **Add Job**.
5. For **Name**, enter **audit**.
6. For **Type**, select D**B2 CLP Script**.
7. Click **OK**.
8. Add script.
9. Add schedule detail to audit task.
10. Add database to audit task.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections 'Discovering Infrastructure' and 'Setting Access Credentials' for Device Discovery under Chapter: Configuring FortiSIEM.

Configuring IBM DB2 Audit on Windows - DB2 side

1. Create a non-admin user on Windows, for example “AoAuditUser” , and set password
2. Login DB2 task center, add the user to DB Users, connect it to database
3. Grant Permission (use Administrator), use commands below
   a. Grant audit permission to db2admin

```
db2 connect to sample user administrator using 'ProspectHills!'
DB2 GRANT EXECUTE ON PROCEDURE SYSPROC.AUDIT_ARCHIVE TO DB2ADMIN
DB2 GRANT EXECUTE ON PROCEDURE SYSPROC.AUDIT_DELIM_EXTRACT TO DB2ADMIN
db2 grant load on database to db2admin
db2 grant secadm on database to db2admin
db2 connect reset
```

   b. Grant query permission to non-admin user

```
db2 connect to sample user db2admin using  'ProspectHills!'
db2 grant select on AUDIT to AOAuditUser
db2 grant select on CHECKING to AOAuditUser
db2 grant select on OBJMAINT to AOAuditUser
db2 grant select on SECMAINT to AOAuditUser
db2 grant select on SYSADMIN to AOAuditUser
db2 grant select on VALIDATE to AOAuditUser
db2 grant select on CONTEXT to AOAuditUser
```

```
db2 grant select on EXECUTE to AOAuditUser
db2 connect reset
```

c. Check permission for non-admin user

```
db2 connect to sample user AOAuditUser using 'ProspectHills!'
db2 select count (*) from DB2ADMIN.AUDIT
db2 select count (*) from DB2ADMIN.CHECKING
db2 select count (*) from DB2ADMIN.OBJMAINT
db2 select count (*) from DB2ADMIN.SECMAINT
db2 select count (*) from DB2ADMIN.SYSADMIN
db2 select count (*) from DB2ADMIN.VALIDATE
db2 select count (*) from DB2ADMIN.CONTEXT
db2 select count (*) from DB2ADMIN.EXECUTE
db2 connect reset
```

4. Create Catalog with db2admin
5. Create task in DB2 user Administrator:
   a. Open DB2 task center, create a task like below
   b. Add schedule
   c. Add task

Settings for Access Credentials

Settings for IBM DB2 JDBC Access Credentials

- Values for **Used For = Audit**
- Values for **Used For = Synthetic Transaction Monitoring**

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device:

Values for Used For = Audit:

Setting	Value
Name	db2_linux
Device Type	IBM DB2
Access Protocol	JDBC
Used For	audit
Pull Interval (minutes)	5
Port	50000
Database Name	<database_name>
Audit Table	AUDIT
Checking Table	CHECKING

Setting	Value
ObjMaint Table	OBJMAINT
SecMaint Table	SECMAINT
SysAdmin Table	SYSADMIN
Validate Table	VALIDATE
Context Table	CONTEXT
Execute Table	EXECUTE
Account Name	The administrative user for your IBM DB2 server
Password	The password associated with the administrative user for your IBM DB2 server

Values for Used For = Synthetic Transaction Monitoring:

Setting	Value
Name	db2_linux
Device Type	IBM DB2
Access Protocol	JDBC
Used For	Synthetic Transaction Monitoring
Pull Interval (minutes)	5
Port	50000
Database Name	<database_name>
Account Name	The administrative user for your IBM DB2 server
Password	The password associated with the administrative user for your IBM DB2 server

Sample Events

```
IBMDB2_CHECKING_OBJECT
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_CHECKING_OBJECT]:[eventSeverity]=PHL_INFO,
[objName]=TABLES,[srcIpAddr]=127.0.0.1,[srcApp]=DB2HMON,[dbName]=SAMPLE,[appVersion]=DB2
v10.1.0.0,[instanceName]=db2inst1,[eventTime]=2014-05-14-13.44.41.085567,[user]=db2inst1,
[eventCategory]=CHECKING,[dbRetCode]=0
IBMDB2_CHECKING_FUNCTION
```

```
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_CHECKING_FUNCTION]:[eventSeverity]=PHL_INFO,
[objName]=CHECKING,[srcIpAddr]=127.0.0.1,[srcApp]=DB2HMON,[dbName]=SAMPLE,[appVersion]=DB2
v10.1.0.0,[instanceName]=db2inst1,[eventTime]=2014-05-14-13.44.40.739649,[user]=db2inst1,
[eventCategory]=CHECKING,[dbRetCode]=0
IBMDB2_STATEMENT
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_STATEMENT]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.48.59.433204,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
IBMDB2_COMMIT
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_COMMIT]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=10.1.2.81,[srcApp]=db2jcc_application,[dbName]=SAMPLE,[appVersion]=DB2
v10.1.0.0,[instanceName]=db2inst1,[eventTime]=2014-05-14-13.51.30.447924,[srcName]=SP81,
[user]=db2inst1,[eventCategory]=EXECUTE,[dbRetCode]=0
IBMDB2_ROLLBACK
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_ROLLBACK]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.43.43.827986,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
IBMDB2_CONNECT
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_CONNECT]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=DB2HMON,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.44.39.991288,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
IBMDB2_CONNECT_RESET
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_CONNECT_RESET]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.43.43.829149,[user]=db2inst1,
[eventCategory]=EXECUTE,[dbRetCode]=0
IBMDB2_CREATE_OBJECT
<134>May 14 13:57:40 10.1.2.68 java: [IBMDB2_CREATE_OBJECT]:[eventSeverity]=PHL_INFO,
[objName]=CAN_MONITOR=CAN_MONITOR_FUNC,[srcIpAddr]=10.1.2.68,[srcApp]=DS_ConnMgt_,
[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,[instanceName]=db2inst1,[eventTime]=2014-05-14-
13.30.14.827242,[srcName]=10.1.2.68,[user]=db2inst1,[eventCategory]=OBJMAINT,[dbRetCode]=0
IBMDB2_JDBC_PULL_STAT
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_JDBC_PULL_STAT]:[eventSeverity]=PHL_INFO,
[reptModel]=DB2,[dbName]=SAMPLE,[instanceName]=db2inst1,[reptVendor]=IBM,[rptIp]=10.1.2.68,
[auditEventCount]=30,[relayIp]=10.1.2.68,[dbEventCategory]=db2inst1.AUDIT,[appGroupName]=IBM
DB2 Server
IBMDB2_ARCHIVE
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_ARCHIVE]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.43.44.002046,[user]=db2inst1,
[eventCategory]=AUDIT,[dbRetCode]=0
IBMDB2_EXTRACT
<134>May 14 13:57:39 10.1.2.68 java: [IBMDB2_EXTRACT]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.38.45.865016,[user]=db2inst1,
[eventCategory]=AUDIT,[dbRetCode]=0
IBMDB2_LIST_LOGS
<134>May 14 14:03:39 10.1.2.68 java: [IBMDB2_LIST_LOGS]:[eventSeverity]=PHL_INFO,
[srcIpAddr]=127.0.0.1,[srcApp]=db2bp,[dbName]=SAMPLE,[appVersion]=DB2 v10.1.0.0,
[instanceName]=db2inst1,[eventTime]=2014-05-14-13.58.43.204054,[user]=db2inst1,
[eventCategory]=AUDIT,[dbRetCode]=0
```

Microsoft SQL Server

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.1

Supported Versions:

- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019

Vendor: Microsoft

Product Information: https://www.microsoft.com/en-us/sql-server/

Supported Versions

- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Microsoft SQL server.

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
WMI		Windows application event logs - successful and failed login	Security Monitoring
JDBC		**General database info**: database name, database version, database size, database owner, database created date, database status, database compatibility level **Database configuration Info**: Configure name, Configure value, Configure max and min value, Configure running value **Database backup Info:** Database name, Last backup date, Days since last backup	Availability Monitoring
JDBC		**Database performance metrics (per-instance):** Buffer cache hit ratio, Log cache hit ratio, Transactions /sec, Page reads/sec, Page writes/sec, Page splits/sec, Full scans/sec, Deadlocks/sec, Log flush waits/sec, Latch waits/sec, Data file(s) size, Log file(s) used, Log growths, Log shrinks, User connections, Target server memory, Total Server Memory, Active database users, Logged-in database users, Available buffer pool pages, Free buffer pool pages, Average wait time **Database performance metrics (per-instance, per-database):** Database name, Data file size, Log file used, Log growths, Log shrinks, Log flush waits/sec, Transaction /sec, Log cache hit ratio	Performance Monitoring
JDBC		**Locking info**: Database id, Database object id, Lock type, Locked resource, Lock mode, Lock status **Blocking info**: Blocked Sp Id, Blocked Login User, Blocked Database, Blocked Command, Blocked Process Name, Blocking Sp Id, Blocking Login User, Blocking Database, Blocking Command, Blocking Process Name, Blocked duration	Performance Monitoring
JDBC		**Database error log** **Database audit trail:**Failed database logon is also collected through performance monitoring as logon failures cannot be collected via database triggers.	Availability / Performance Monitoring
JDBC	None	**Database audit trail:** Successful and failed	Security Monitoring

Protocol	Information discovered	Metrics collected	Used for
		database logon, Various database operation audit trail including CREATE/ALTER/DROP/TRUNCATE operations on tables, table spaces, databases, clusters, users, roles, views, table indices, triggers etc	and compliance

Recommended Configuration

1. SNMP or WMI for discovery and system level performance metrics
2. FortiSIEM Windows Agent for Database Audit logs – Note that these logs can also be pulled via WMI, however performance is limited because of WMI limitations.
3. JDBC for Database Performance metrics
4. JDBC for DDL changes

SNMP Configuration

See SNMP Configurations in the *Microsoft Windows Server Configuration* section.

WMI Configuration

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

Configuration for Database Audit Logs

Database Audit logs include failed and successful logons and other C2 audit activity. These logs are written to the Windows Application logs.

Configuration occurs in two parts.

- SQL Server Configuration
- FortiSIEM Configuration

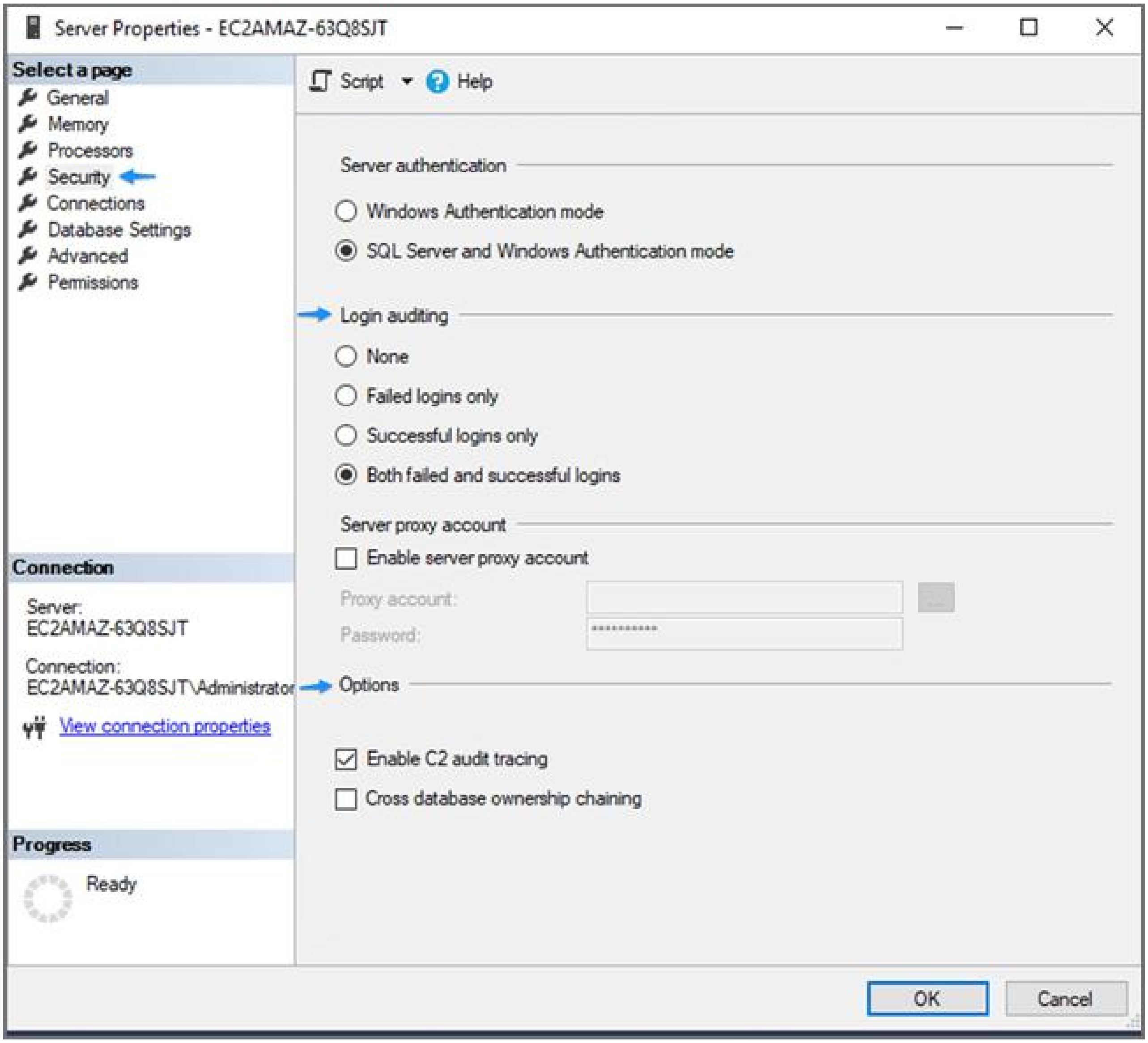
SQL Server Configuration

Step 1: Configure Login Auditing using SQL Server Management studio

Take the following steps to configure Login Auditing.

1. In SQL Server Management Studio, connect to an instance of the SQL Server Database Engine with Object Explorer.
2. In Object Explorer, right-click the server name, and then click **Properties**.
3. On the **Security** page, under **Login auditing**, select the desired option

4. On the **Security** page, under **Options**, click on the **Enable C2 audit tracing** check box and close the **Server Properties** page.
5. In Object Explorer, right-click the server name, and then click **Restart**.



Server: EC2AMAZ-63Q8SJT

Connection: EC2AMAZ-63Q8SJT\Administrator

Server authentication

○ Windows Authentication mode
● SQL Server and Windows Authentication mode

Login auditing

○ None
○ Failed logins only
○ Successful logins only
● Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: ***********

Options

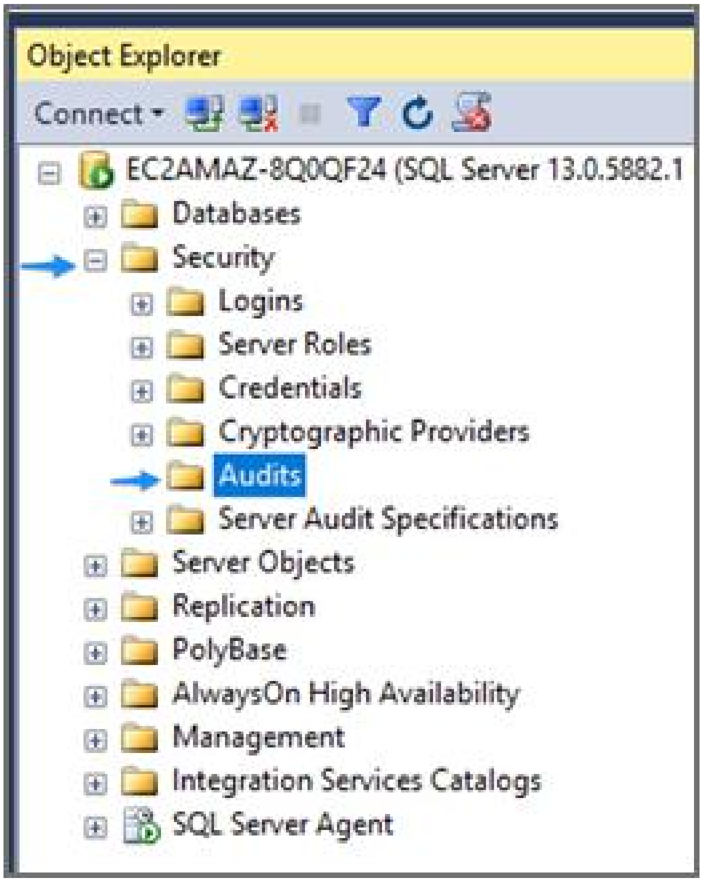
☑ Enable C2 audit tracing
□ Cross database ownership chaining

Note: You must **restart** the SQL Server before this option will take effect.

Step 2: Enabling SQL Server Audit

Create a Server-level audit object by taking the following steps:

1. In SQL Server Management Studio, connect to an instance of the SQL Server Database Engine with Object Explorer.
2. In the Object Explorer panel on the left, expand **Security**.
3. Right-click **Audits**, and select **New Audit…** from the menu. This will create a new SQL Server Audit object for server-level auditing.

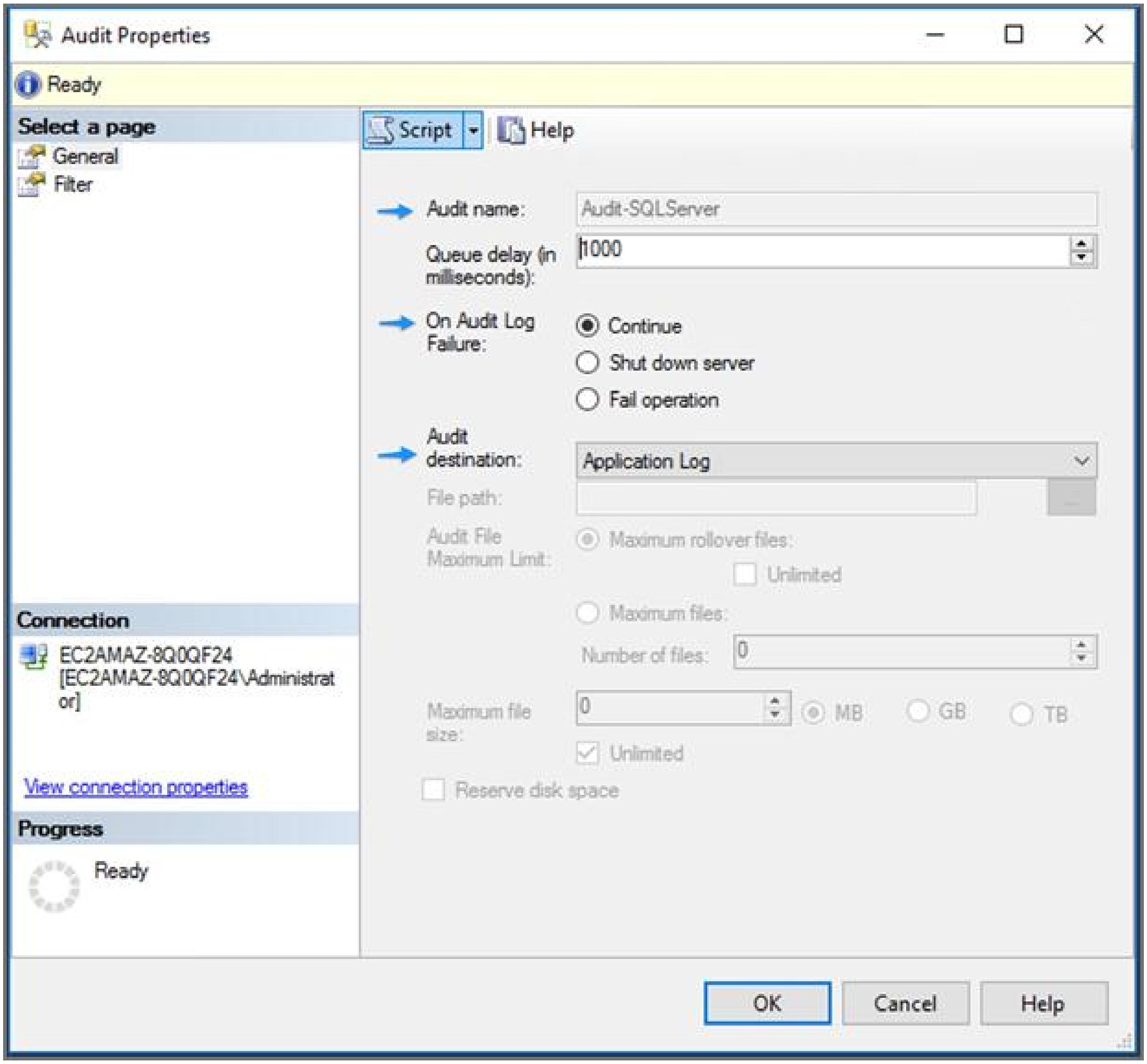


Object Explorer

Connect ▾

- EC2AMAZ-8Q0QF24 (SQL Server 13.0.5882.1
  - Databases
  - Security
    - Logins
    - Server Roles
    - Credentials
    - Cryptographic Providers
    - Audits
    - Server Audit Specifications
  - Server Objects
  - Replication
  - PolyBase
  - AlwaysOn High Availability
  - Management
  - Integration Services Catalogs
  - SQL Server Agent

4. In the Create Audit window, give the audit settings a name in the **Audit name** field.
5. For **On Audit Log Failure**, select the **Continue** option.
6. For **Audit destination**, select **Application Log** from the drop-down list.



Audit name: Audit-SQLServer

Queue delay (in milliseconds): 1000

On Audit Log Failure: ● Continue ○ Shut down server ○ Fail operation

Audit destination: Application Log

File path:

Audit File Maximum Limit: ● Maximum rollover files: □ Unlimited ○ Maximum files:

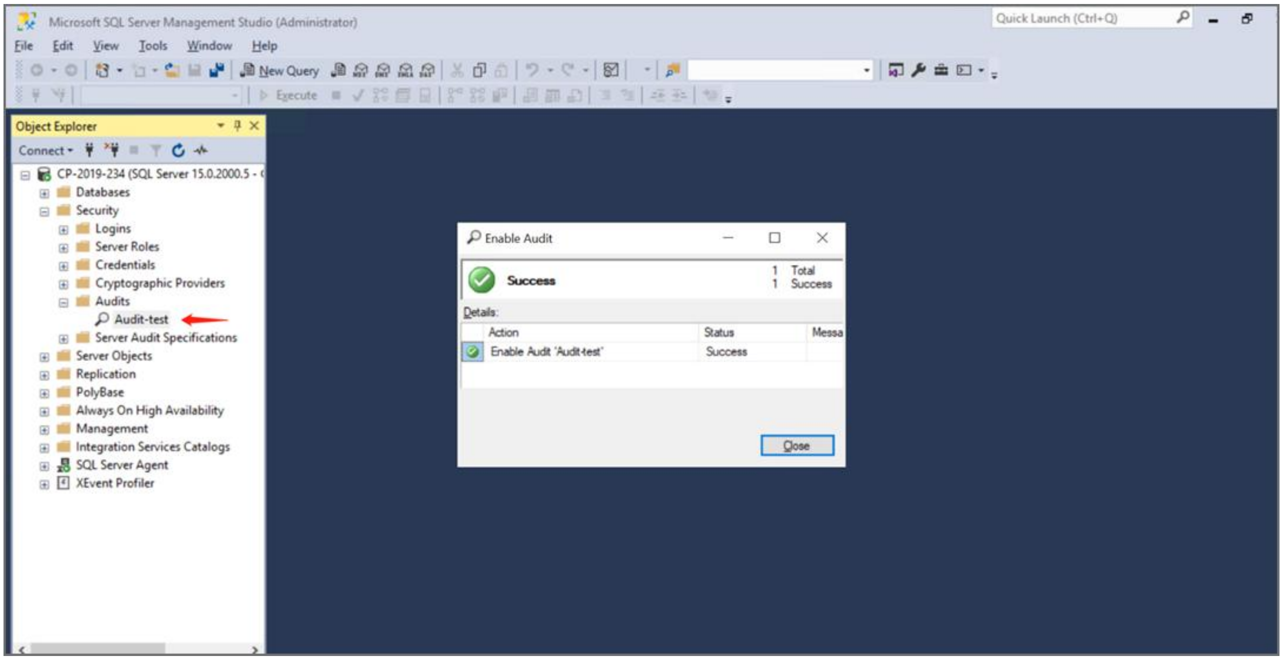
Number of files: 0

Maximum file size: 0 ● MB ○ GB ○ TB ☑ Unlimited

□ Reserve disk space

EC2AMAZ-8Q0QF24 [EC2AMAZ-8Q0QF24\Administrator]

7. Click **OK**.
8. You will now find the new audit configuration in Object Explorer below Security > Audits. Right-click the new Audit configuration and select **Enable Audit** from the menu.



Success

1 Total
1 Success

Details:

Action	Status	Messa
Enable Audit 'Audit-test'	Success	

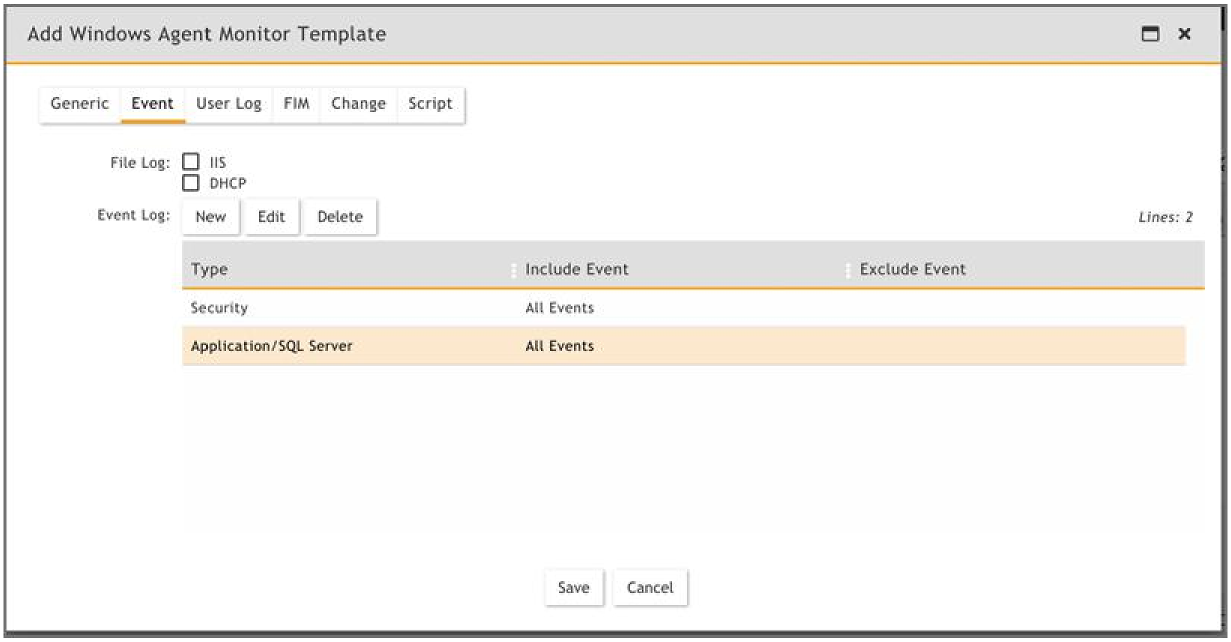
9. Click **Close** in the Enable Audit dialog.

FortiSIEM Configuration

Step1: Define the Windows Agent Monitor Template for SQL Server

Complete these steps to add a Windows Agent Monitor Template:

1. Navigate to **ADMIN > Setup** and click the **Windows Agent** tab.
2. Under **Windows Agent Monitor Templates** click **New**.
3. In the **Windows Agent Monitor Template** dialog box, in the **Name** field, enter a name.
4. Click on **Event** tab, and take following steps:
    a. In the **Event Log** row, click **New**.
    b. From the **Type** drop-down list, select **Security** and click **Save**.
    c. In the **Event Log** row, click **New** again.
    d. From the **Type** drop-down list, select **Application**.
    e. From the **Source** drop-down list, select **SQL Server**.
    f. Click **Save**.



File Log: □ IIS
□ DHCP

Event Log:

Lines: 2

Type	Include Event	Exclude Event
Security	All Events	
Application/SQL Server	All Events	

Step 2: Associate Windows Agents to Templates

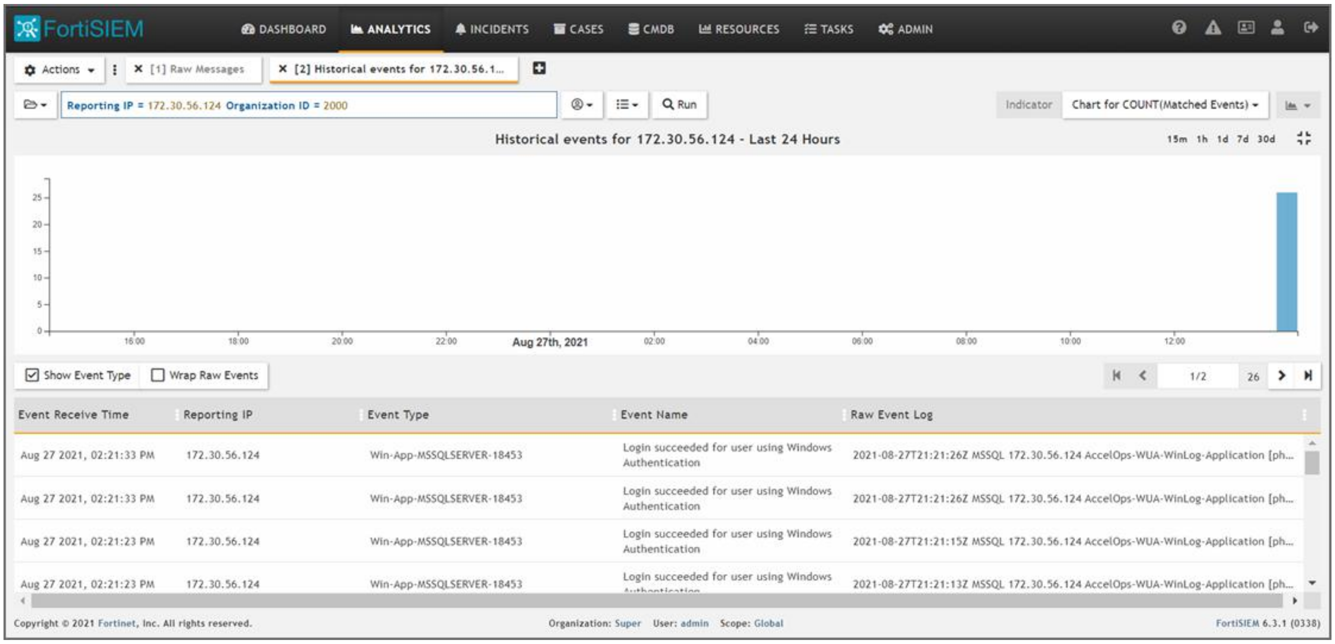
Complete these steps to associate a Host to Template:

1. Under **Host To Template Associations**, click **New**.
2. In the **Host To Template Associations** dialog box, enter the following information.

Settings	Guidelines
Name	Name of the Host to Template Association.
Organization	Select the organization.
Host	Use the drop-down list to browse the folders and select the **Devices** or/and **Business Services** to monitor and click **Save**.
Template	Select one or more monitoring templates from the list, or select All Templates to include all. You can also use the serarch bar to find any specific template.
Collector	Select the Collector from the list or select **All Collectors** to include all. Agents forward events to Collectors via HTTP(S). A Collector is chosen at random and if that Collector is not available or non-responive, then another Collector in the list is chosen.

3. Associate the recently added SQL Server template to SQL server host.
4. Click **Save and Apply**.

Step 3: Check Events via Analytics



Reporting IP = 172.30.56.124 Organization ID = 2000

Historical events for 172.30.56.124 - Last 24 Hours

Event Receive Time	Reporting IP	Event Type	Event Name	Raw Event Log
Aug 27 2021, 02:21:33 PM	172.30.56.124	Win-App-MSSQLSERVER-18453	Login succeeded for user using Windows Authentication	2021-08-27T21:21:26Z MSSQL 172.30.56.124 AccelOps-WUA-WinLog-Application [ph...
Aug 27 2021, 02:21:33 PM	172.30.56.124	Win-App-MSSQLSERVER-18453	Login succeeded for user using Windows Authentication	2021-08-27T21:21:26Z MSSQL 172.30.56.124 AccelOps-WUA-WinLog-Application [ph...
Aug 27 2021, 02:21:23 PM	172.30.56.124	Win-App-MSSQLSERVER-18453	Login succeeded for user using Windows Authentication	2021-08-27T21:21:15Z MSSQL 172.30.56.124 AccelOps-WUA-WinLog-Application [ph...
Aug 27 2021, 02:21:23 PM	172.30.56.124	Win-App-MSSQLSERVER-18453	Login succeeded for user using Windows Authentication	2021-08-27T21:21:13Z MSSQL 172.30.56.124 AccelOps-WUA-WinLog-Application [ph...

Copyright © 2021 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM 6.3.1 (0338)

JDBC Configuration for Database Performance Metrics

FortiSIEM can pull SQL Server performance metrics via JDBC.

Configuration occurs in two parts.

- SQL Server Configuration
- FortiSIEM Configuration

SQL Server Configuration

Step 1: Create a Read-Only User for SQL Server Monitoring

A regular Windows account cannot be used for SQL Server monitoring. FortiSIEM runs on Linux and certain Windows libraries needed for SQL Server monitoring are not available on Linux. You have to create a separate user with read-only privileges.

1. Log in to your SQL Server with sa account, and then create a read-only user to access system tables.

```
EXEC SP_ADDLOGIN 'AOPerfLogin','ProspectHills!','master';
EXEC SP_ADDROLE 'AOPerfRole';
EXEC SP_ADDUSER 'AOPerfLogin', 'AOPerfUser', 'AOPerfRole';
GRANT VIEW SERVER STATE TO AOPerfLogin;
GRANT SELECT ON dbo.sysperfinfo TO AOPerfRole;
GRANT EXEC on xp_readerrorlog to AOPerfRole;
```

2. Log in with your newly created read-only account (AOPerfLogin) and run these commands.

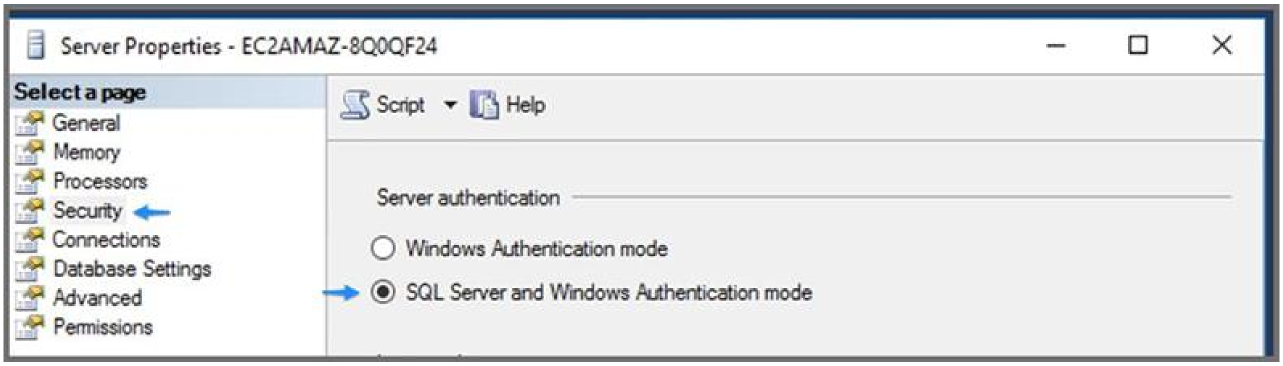
```
SP_WHO2 'active';
SELECT * FROM sys.databases; SELECT * FROM dbo.sysperfinfo;
SELECT COUNT(*) as count FROM sysprocesses GROUP BY loginame;
```

Check to see if you get the same results with your read-only account (AOPerfLogin) as you do with your sa account. You should get the same results.

Step 2: Changing Authentication mode to SQL Server and Windows Authentication Mode

It is common practice to enable SQL Server and Windows Authentication mode before accessing read-only user. To enable this mode, take the following steps:

1. In **SQL Server Management Studio Object Explorer**, right click the server, then click **Properties**.
2. On the **Security** page, under **Sever authentication**, select **SQL Server and Windows Authentication mode**.



3. Click **OK**.
4. In the **SQL Server Management Studio** dialog box, click **OK** to acknowledge the requirement to **restart** the SQL Server.
5. In **Object Explorer**, right click your server, and then click **Restart**. If the SQL Server Agent is running, it must also be restarted.

FortiSIEM Configuration

Settings for SQL Server JDBC Access Credentials for Performance Monitoring

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your SQL Server over JDBC for performance monitoring:

Step 1: Create a Separate Credential for Each Database Instance

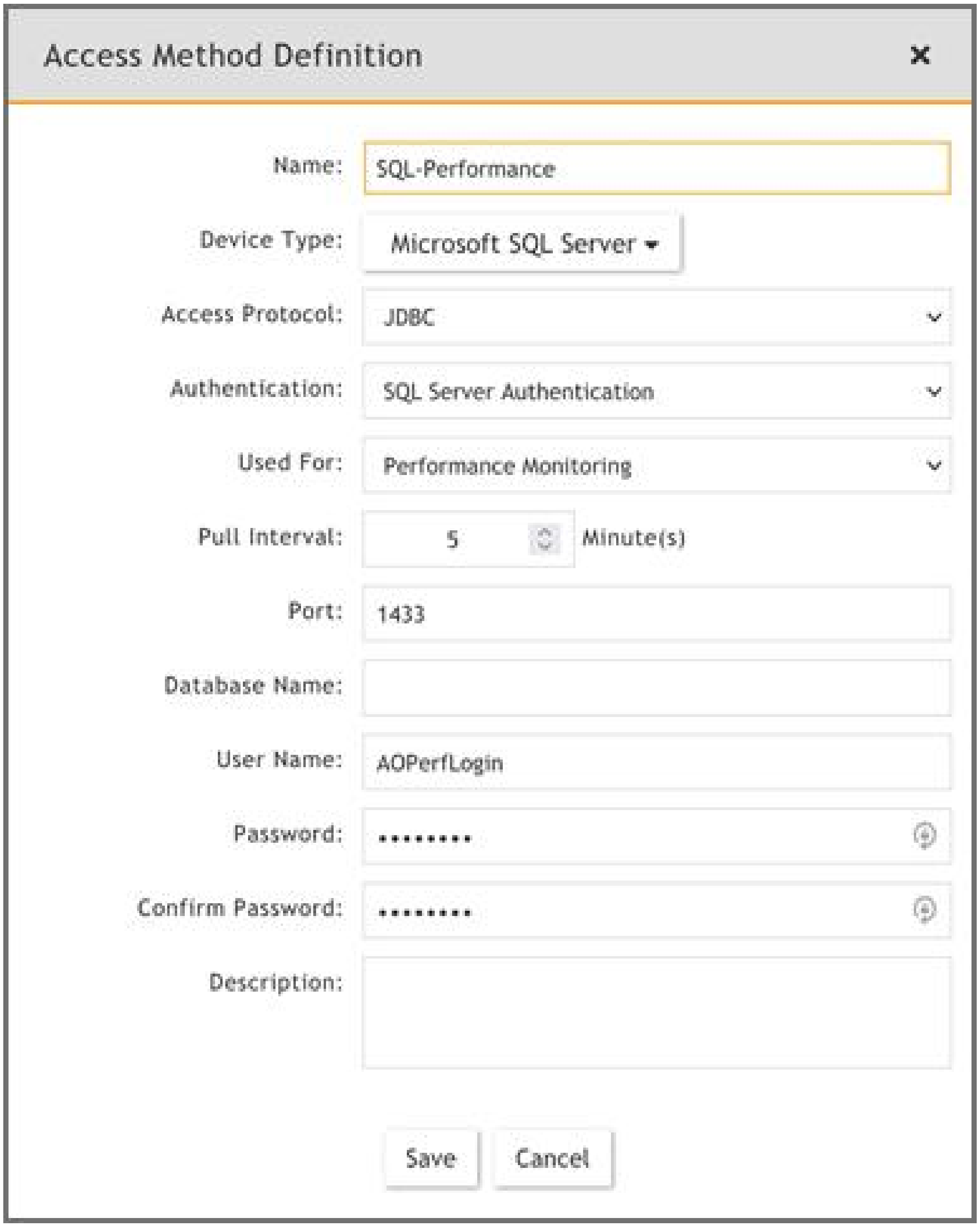
If multiple database instances are running on the same server, then each instance must run on a separate port, and you must create a separate access credential for each instance. You must also remember to associate each instance with the server's IP number for the **Device Credential Mapping Definition**.

Take the following steps:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the **Access Method Definition** dialog box and click **Save** when done:

i.

Setting	Value
Name	The name of the database instance you're creating the credential for.
Access Protocol	JDBC
Used For	Performance Monitoring
Pull Interval (minutes)	5
Port	1433
Database Name	<leave this field blank>
User Name	The user you created in step 1 of the JDBC configuration.
Password	The password associated with the user you created in step 1.



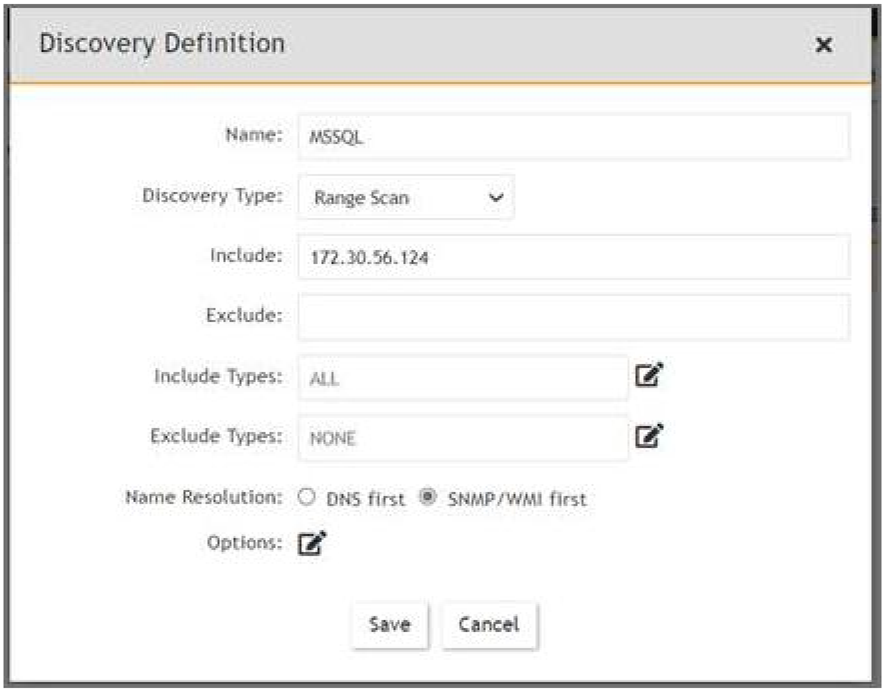
Access Method Definition

Name:	SQL-Performance
Device Type:	Microsoft SQL Server
Access Protocol:	JDBC
Authentication:	SQL Server Authentication
Used For:	Performance Monitoring
Pull Interval:	5 Minute(s)
Port:	1433
Database Name:	
User Name:	AOPerfLogin
Password:	••••••••
Confirm Password:	••••••••
Description:	

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   - a. Select the name of your credential from the **Credentials** drop-down list.
   - b. In the **IP/Host Name** field, enter a host name, an IP, or an IP range.
   - c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the Microsoft SQL Server.
5. To discover the device, take the following steps:
   - a. Navigate to **ADMIN > Setup > Discovery**.
   - b. Create a Discovery entry using the information here. For more information on how to create a discovery entry, see here.

Setting	Value
Name	The name of the device to discover
Discovery Type	Leave as default (Range Scan).
Include	Provide the IP address of the device you want discovered.

c. Click **Save** when done.



Discovery Definition

Name: MSSQL

Discovery Type: Range Scan

Include: 172.30.56.124

Exclude:

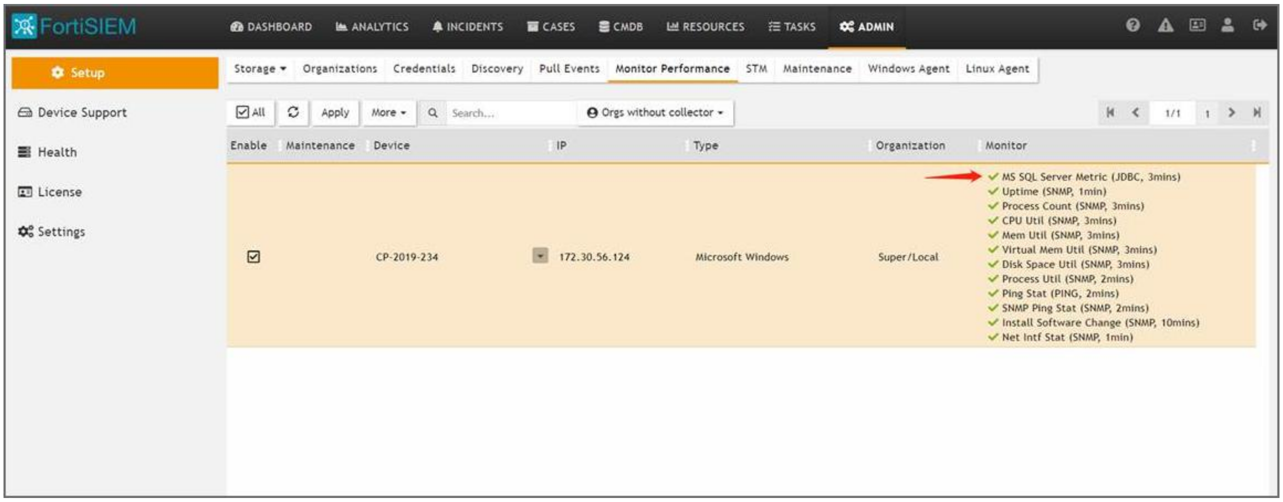
Include Types: ALL

Exclude Types: NONE

Name Resolution: ○ DNS first ● SNMP/WMI first

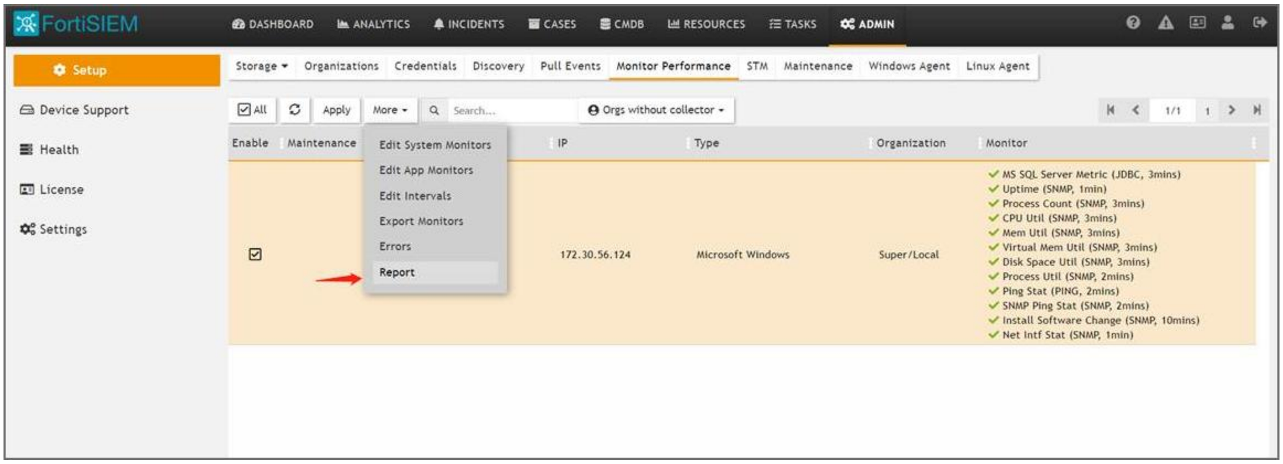
Options:

6. Select the discovery entry you created and click **Discover**.
7. After Discovery is completed, navigate to **ADMIN > Setup > Monitor Performance** to check the monitor performance job.



Enable	Maintenance	Device	IP	Type	Organization	Monitor
☑		CP-2019-234	172.30.56.124	Microsoft Windows	Super/Local	✓ MS SQL Server Metric (JDBC, 3mins) ✓ Uptime (SNMP, 1min) ✓ Process Count (SNMP, 3mins) ✓ CPU Util (SNMP, 3mins) ✓ Mem Util (SNMP, 3mins) ✓ Virtual Mem Util (SNMP, 3mins) ✓ Disk Space Util (SNMP, 3mins) ✓ Process Util (SNMP, 2mins) ✓ Ping Stat (PING, 2mins) ✓ SNMP Ping Stat (SNMP, 2mins) ✓ Install Software Change (SNMP, 10mins) ✓ Net Intf Stat (SNMP, 1min)

8. Click on the **More** drop-down list and select **Report** to check related events.



Enable	Maintenance	IP	Type	Organization	Monitor
☑		172.30.56.124	Microsoft Windows	Super/Local	✓ MS SQL Server Metric (JDBC, 3mins) ✓ Uptime (SNMP, 1min) ✓ Process Count (SNMP, 3mins) ✓ CPU Util (SNMP, 3mins) ✓ Mem Util (SNMP, 3mins) ✓ Virtual Mem Util (SNMP, 3mins) ✓ Disk Space Util (SNMP, 3mins) ✓ Process Util (SNMP, 2mins) ✓ Ping Stat (PING, 2mins) ✓ SNMP Ping Stat (SNMP, 2mins) ✓ Install Software Change (SNMP, 10mins) ✓ Net Intf Stat (SNMP, 1min)

JDBC Configuration for DDL Changes

FortiSIEM can pull SQL Server Data Definition Language (DDL) changes via JDBC. These changes include CREATE, ALTER, DROP, GRANT, DENY, REVOKE or UPDATE STATISTICS operations on database tables. This information is not naturally generated by a SQL Server. Hence, this involves creating database tables to store them and then creating triggers to populate those tables. Then FortiSIEM can pull them via JDBC.

Configuration occurs in two parts.

- SQL Server Configuration
- FortiSIEM Configuration

SQL Server Configuration

1. Save the SQL Server script (provided – link here) as separate file to **My Documents > SQL Server Management Studio > SQLServer_DDL_Events.sql**.
2. Login to SQL Server Management Studio with *sa account*.
3. Browse to and execute the **SQLServer_DDL_Events.sql** script to create the database, tables and trigger events.

Creating a Database Truncate Script

Since DDL tables grow after time, it is often a good idea to create a database truncate script that can run as a maintenance task and keep the table size under control. it is often necessary to create a database truncate procedure as follows.

1. Log into Microsoft SQL Management Studio and connect to the DB instance.
2. Under **Management**, go to **Maintenance Plans**, and create a new plan with the name **RemoveOldLogs**.
3. For **Subplan**, enter **TRUNCATE**, and for **Description**, enter **TRUNCATE TABLE**.
4. Click the **Calendar** icon to create a recurring, daily task starting at 12:00AM and running every 30 minutes until 11:59:59PM.
5. Go to **View > Tool Box > Execute T-SQL Statement**. A T-SQL box will be added to the subplan.
6. In the T-SQL box, enter this command

```
use PH_Events;
EXEC sp_MSForEachTable 'TRUNCATE TABLE DDLEvents';
```

7. Click OK.

You will be able to see the history of this script's actions by right-clicking on the maintenance task, and then selecting **View History**.

FortiSIEM Configuration

Settings for SQL Server JDBC Access Ccredentials for DDL Events Collection

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your SQL Server database instance over JDBC for database DDL events collection.

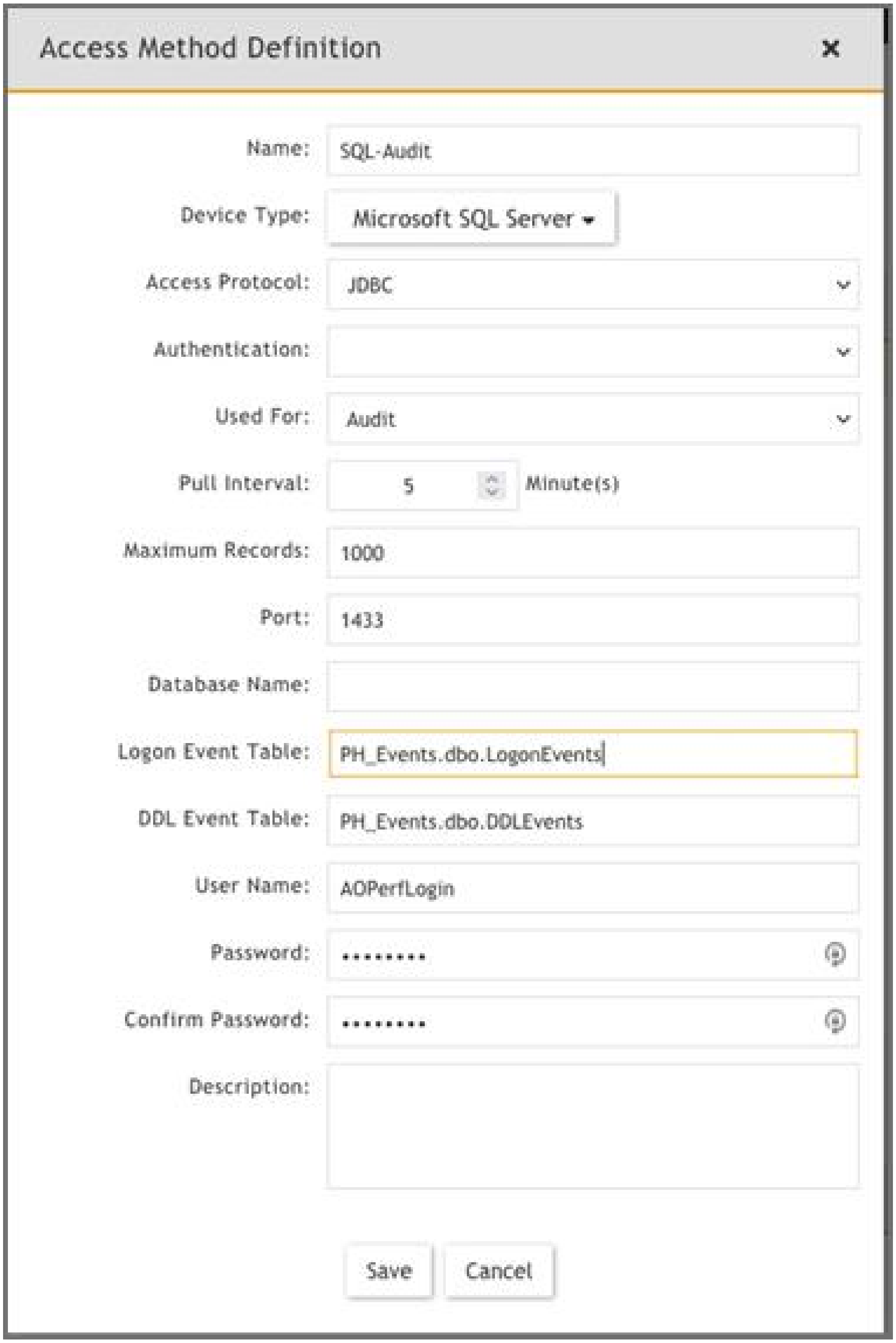
Step 1: Create a Separate Credential for Each Database Instance

If multiple database instances are running on the same server, then each instance must run on a separate port, and you must create a separate access credential for each instance. You must also remember to associate each instance with the server's IP number for the **Device Credential Mapping Definition**.

Take the following steps:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the **Access Method Definition** dialog box, and click **Save** when done:

Setting	Value
Name	The name of the database instance you are creating the credential for
Device Type	Microsoft SQL Server
Used For	Audit
Pull Interval (minutes)	5
Port	1433
Database Name	<leave this field blank>
Logon Event Table	PH_Events.dbo.LogOnEvents
DDL Event Table	PH_Events.dbo.DDLEvents
User Name	The user you created in step 1 of the JDBC configuration
Password	The password associated with the user you created in step 1.



Access Method Definition

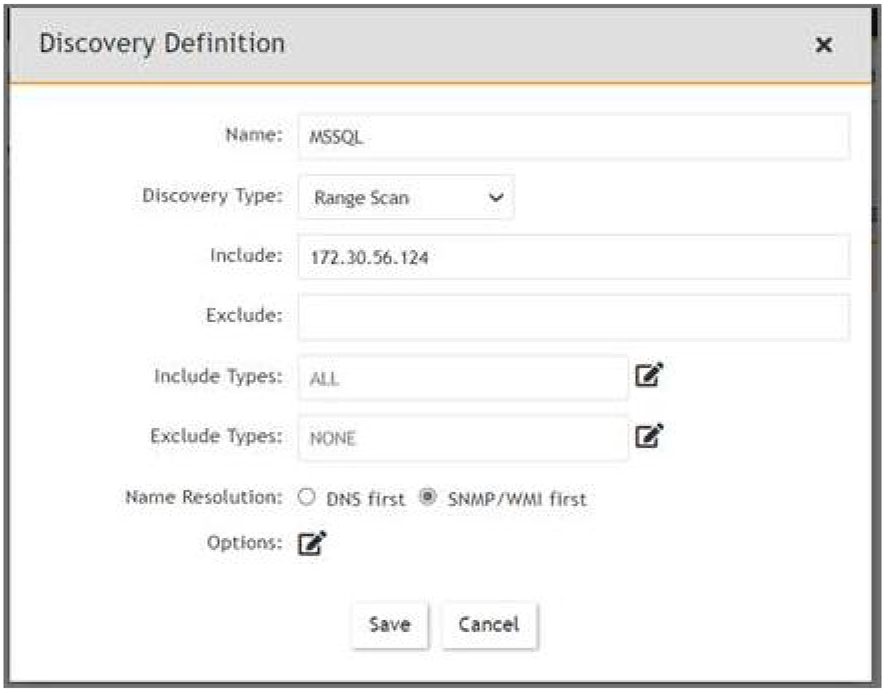
Name:	SQL-Audit
Device Type:	Microsoft SQL Server
Access Protocol:	JDBC
Authentication:	
Used For:	Audit
Pull Interval:	5 Minute(s)
Maximum Records:	1000
Port:	1433
Database Name:	
Logon Event Table:	PH_Events.dbo.LogonEvents
DDL Event Table:	PH_Events.dbo.DDLEvents
User Name:	AOPerfLogin
Password:	••••••••
Confirm Password:	••••••••
Description:	

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Select the name of your credential from the **Credentials** drop-down list.
   b. In the **IP/Host Name** field, enter a host name, an IP, or an IP range.
   c. Click **Save**.

4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the Microsoft SQL Server.
5. To discover the device, take the following steps:
   a. Navigate to **ADMIN > Setup > Discovery**.
   b. Create a Discovery entry using the information here. For more information on how to create a discovery entry, see here.

Setting	Value
Name	The name of the device to discover
Discovery Type	Leave as default (Range Scan).
Include	Provide the IP address of the device you want discovered.

   c. Click **Save** when done.



Discovery Definition

Name: MSSQL

Discovery Type: Range Scan

Include: 172.30.56.124

Exclude:

Include Types: ALL

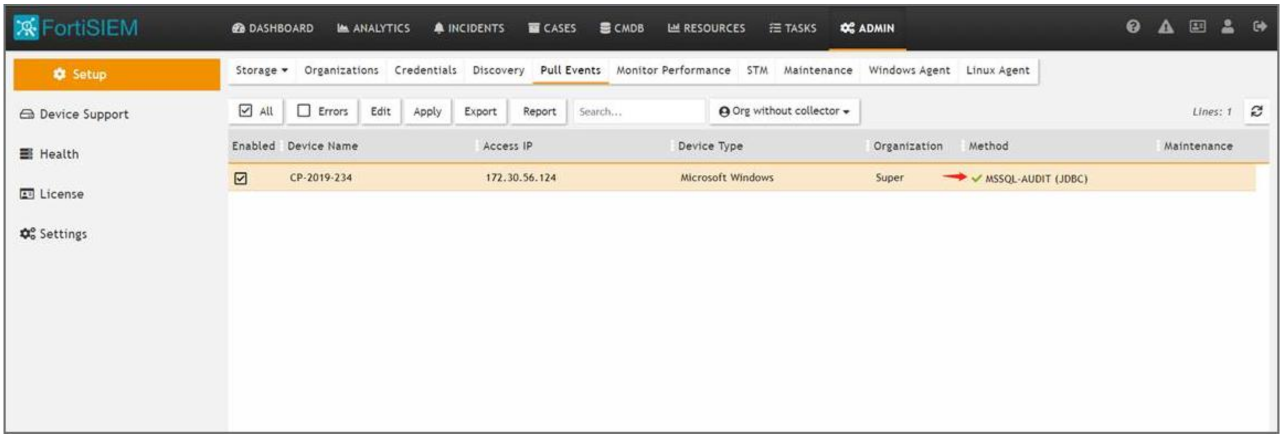
Exclude Types: NONE

Name Resolution: ○ DNS first ● SNMP/WMI first

Options:

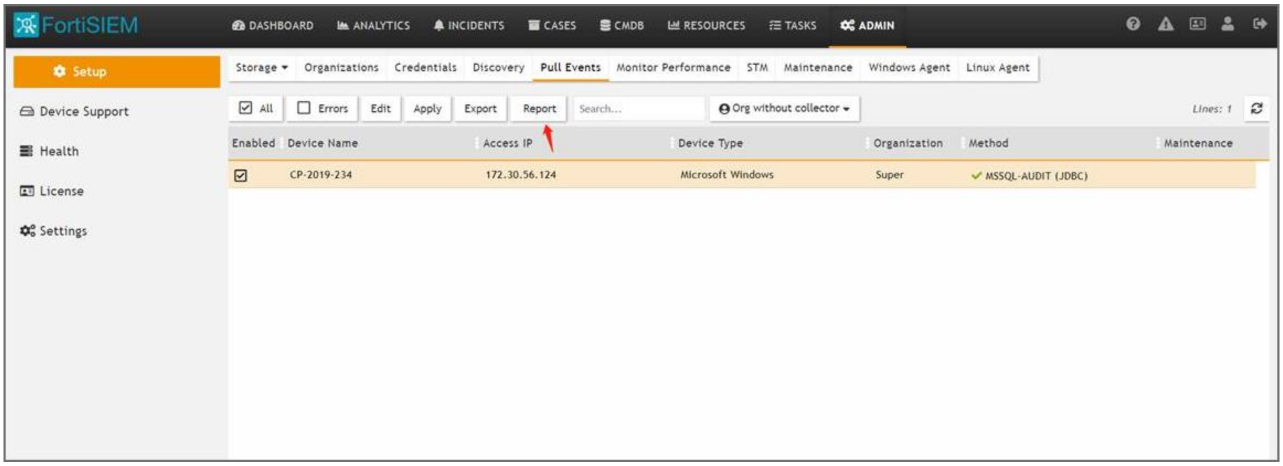
6. Select the discovery entry you created and click **Discover**.

7. After Discovery is completed, navigate to **ADMIN > Setup > Pull Events** to check the pull events job.



Enabled	Device Name	Access IP	Device Type	Organization	Method	Maintenance
☑	CP-2019-234	172.30.56.124	Microsoft Windows	Super	✓ MSSQL-AUDIT (JDBC)	

8. Click on **Report** to check related events.



Enabled	Device Name	Access IP	Device Type	Organization	Method	Maintenance
☑	CP-2019-234	172.30.56.124	Microsoft Windows	Super	✓ MSSQL-AUDIT (JDBC)	

Sample Events

- Per Instance Performance Metrics
- Per Instance, per Database Performance Metrics
- Generic Info
- Config Info
- Locking Info
- Blocking Info
- Error Log
- Logon Events
- DDL Events - Create Database
- DDL Events - Create Index

Per Instance Performance Metrics

```
<134>Apr 16 10:17:56 172.16.22.100 java: [PH_DEV_MON_PERF_MSSQL_SYS|PH_DEV_MON_PERF_MSSQL_
SYS]:[eventSeverity]=PHL_INFO,[hostIpAddr]=172.16.22.100,[hostName]=wwwin.accelops.net,
[appGroupName]=Microsoft SQL Server,[dbDataFileSizeKB]=13149056,[dbLogFileUsedKB]=26326,
[dbLogGrowthCount]=4,[dbLogShrinkCount]=0,[dbLogFlushPerSec]=1.69,[dbTransPerSec]=4.44,
[dbDeadLocksPerSec]=0,[dbLogCacheHitRatio]=60.01,[dbUserConn]=16,
[dbTargetServerMemoryKB]=1543232,[dbTotalServerMemoryKB]=1464760,[dbPageSplitsPerSec]=0.45,
[dbPageWritesPerSec]=0.01,[dbLatchWaitsPerSec]=0.77,[dbPageReadsPerSec]=0.01,
[dbFullScansPerSec]=1.83,[dbBufferCacheHitRatio]=100,[dbCount]=8,[dbUserCount]=25,
[dbLoggedinUserCount]=2,[dbPagesInBufferPool]=116850,[dbPagesFreeInBufferPool]=2336,
[dbAverageWaitTimeMs]=239376,
[appVersion]=Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64),[serverName]=WIN-08-
VCENTER,[instanceName]=MSSQLSERVER,[appPort]=1433
```

Per Instance, per Database Performance Metrics

```
[PH_DEV_MON_PERF_MSSQL_PERDB]:[eventSeverity]=PHL_INFO,[hostIpAddr]=172.16.22.100,
[hostName]=wwwin.accelops.net,[dbName]=tempdb,[appGroupName]=Microsoft SQL Server,
[dbDataFileSizeKB]=109504,[dbLogFileUsedKB]=434,[dbLogGrowthCount]=4,[dbLogShrinkCount]=0,
[dbTransPerSec]=0.96,[dbLogFlushPerSec]=0.01,[dbLogCacheHitRatio]=44.44,
[appVersion]=Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64),[serverName]=WIN-08-
VCENTER,[instanceName]=MSSQLSERVER,[appPort]=1433
```

Generic Info

```
[PH_DEV_MON_PERF_MSSQL_GEN_INFO]:[eventSeverity]=PHL_INFO,[dbName]= tempdb,[dbSize]= 3.0,
[dbowner]= sa,[dbId]= 2,[dbcreated]= 1321545600,
[dbstatus]= Status=ONLINE; Updateability=READ_WRITE; UserAccess=MULTI_USER; Recovery=SIMPLE;
Version=655; Collation=SQL_Latin1_General_CP1_CI_AS; SQLSortOrder=52;
IsAutoCreateStatistics; IsAutoUpdateStatistics,
[dbcompatibilityLevel]= 100,[spaceAvailable]= 0.9,[appVersion]= Microsoft SQL Server 2008
(RTM) - 10.0.1600.22 (Intel X86),[serverName]= WIN03MSSQL\SQLEXPRESS
```

Config Info

```
[PH_DEV_MON_PERF_MSSQL_CONFIG_INFO]:[eventSeverity]=PHL_INFO,[configureName]= user instances
enabled,[configMinimum]= 0,[configMaximum]= 1,[dbConfigValue]= 1,
[configRunValue]= 1,[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel
X86),[serverName]= WIN03MSSQL\SQLEXPRESS
```

Locking Info

```
[PH_DEV_MON_PERF_MSSQL_LOCK_INFO]:[eventSeverity]=PHL_INFO,[dbId]= 4,[objId]= 1792725439,
[lockType]= PAG,[lockedResource]= 1:1256,[lockMode]= IX,
[lockStatus]= GRANT,[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel
X86),[serverName]= WIN03MSSQL\SQLEXPRESS
```

Blocking Info

```
[PH_DEV_MON_PERF_MSSQL_BLOCKBY_INFO]:[eventSeverity]=PHL_INFO,[blockedSpId]= 51,
[blockedLoginUser]= WIN03MSSQL\Administrator,[blockedDbName]= msdb,
[blockedCommand]= UPDATE,[blockedProcessName]= Microsoft SQL Server Management Studio -
Query,[blockingSpId]= 54,[blockingLoginUser]= WIN03MSSQL\Administrator,
[blockingDbName]= msdb,[blockingCommand]= AWAITING COMMAND,[blockingProcessName]= Microsoft
SQL Server Management Studio - Query,[blockedDuration]= 5180936,
[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86),[serverName]=
WIN03MSSQL\SQLEXPRESS
```

Error Log

```
[PH_DEV_MON_PERF_MSSQL_ERROR_LOG_INFO]:[eventSeverity]=PHL_INFO,[logDate]= 1321585903,
[processInfo]= spid52,[logText]= Starting up database 'ReportServer$SQLEXPRESSTempDB'.,
[appVersion]= Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86),[serverName]=
WIN03MSSQL\SQLEXPRESS
```

Logon Events

```
134>Feb 08 02:55:34 10.1.2.54 java: [MSSQL_Logon_Success]:[eventSeverity]=PHL_INFO,
[eventTime]=2014-02-08 02:54:00.977, [rptIp]=10.1.2.54, [relayIp]=10.1.2.54,
[srcName]=<local machine>, [user]=NT SERVICE\ReportServer$MSSQLSERVEJIANFA, [srcApp]=Report
Server, [instanceName]=MSSQLSERVEJIANFA, [procId]=52, [loginType]=Windows (NT) Login,
[securityId]=AQYAAAAAAAVQAAAALJAZf5XMbcLh8PUDY31LioZ3Uwo=, [isPooled]=1, [destName]=WIN-
S2EDLFIUPQK, [destPort]=1437,
```

DDL Events - Create Database

```
<134>Sep 29 15:34:48 10.1.2.54 java: [MSSQL_Create_database]:[eventSeverity]=PHL_INFO,
[eventTime]=2013-09-29 15:34:05.687, [rptIp]=10.1.2.54, [relayIp]=10.1.2.54, [user]=WIN-
S2EDLFIUPQK\Administrator, [dbName]=JIANFA, [instanceName]=MSSQLSERVER, [objName]=,
[procId]=59, [command]=CREATE DATABASE JIANFA, [destName]=WIN-S2EDLFIUPQK, [destPort]=1433,
```

DDL Events - Create Index

```
<134>Sep 29 15:34:48 10.1.2.54 java: [MSSQL_Create_index]:[eventSeverity]=PHL_INFO,
[eventTime]=2013-09-29 15:30:40.557, [rptIp]=10.1.2.54, [relayIp]=10.1.2.54, [user]=WIN-
S2EDLFIUPQK\Administrator, [dbName]=master, [instanceName]=MSSQLSERVER, [objName]=IndexTest,
[procId]=58, [command]=create index IndexTest on dbo.MSreplication_options(optname);,
[schemaName]=dbo, [objType]=INDEX, [destName]=WIN-S2EDLFIUPQK, [destPort]=1433
```

MySQL Server

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.0

Supported Versions: :

- MySQL 5.7 and earlier
- MySQL 8.0

Vendor: Oracle

Product Information: https://www.mysql.com/products/

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
JDBC		**Generic database information**: Version, Character Setting	
JDBC		**Database performance metrics:** User Connections, Table Updates, table Selects, Table Inserts, Table Deletes, Temp Table Creates, Slow Queries, Query cache Hits, Queries registered in cache, Database Questions, Users, Live Threads **Table space performance metrics**: Table space name, table space type, Character set and Collation, table space usage, table space free space, Database engine, Table version, Table Row Format, Table Row Count, Average Row Length, Index File length, Table Create time, Table Update Time	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
JDBC	None	**Database audit trail:** Successful and failed database log on, Database CREATE/DELETE/MODIFY operations, Table CREATE/DELETE/MODIFY/INSERT operations	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "mysql" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "mysql" in the main content panel **Search...** field to see the rules associated with this application or device.

Reports

In **RESOURCES > Reports**, search for ""mysql" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- SNMP
- JDBC for Database Auditing - MySQL Server

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

JDBC for Database Auditing - MySQL Server

You must configure your MySQL Server to write audit logs to a database table. This topic in the MySQL documentation explains more about how to set the destination tables for log outputs.

Take the following steps based on your version of Linux:

1. If the binary `bin/mysqld_safe` exists in your version of Linux, run the following command and proceed to step 2:

   ```
   bin/mysqld_safe --user=mysql --log-output=TABLE &
   ```

   If the binary `bin/mysqld_safe` does not exist in your version of Linux, then take the following step based on the version of MySQL being used, then proceed to step 2.
   Note: Some Linux variants that use `systemd`, for example, CentOS, do not contain `bin/mysqld_safe`.

   For MySQL 5.7 and earlier, add the following into `/etc.my.cnf`.

```
log-output=TABLE
```

For MySQL 8.0 and later, add the following into `/etc/my.cnf.d/mysql-server.cnf`.

```
log-output=TABLE
```

2. Login to MySQL, and run the following SQL commands to enable general.log in MyISAM.

```
SET @old_log_state = @@global.general_log;
SET GLOBAL general_log = 'OFF';
ALTER TABLE mysql.general_log ENGINE = MyISAM;
SET GLOBAL general_log = @old_log_state;
SET GLOBAL general_log = 'ON';
```

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide. Use the settings in Settings for MySQL Server JBDC Access Credentials for Database Auditing to set up MySQL Audit.

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Settings for MySQL Server JBDC Access Credentials for Performance Monitoring
- Settings for MySQL Server JBDC Access Credentials for Database Auditing
- Settings for MySQL Server JBDC Access Credentials for Synthetic Transaction Monitoring, Snort Audit, McAfee VulnMgr

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<*set name*>
Device Type	Generic
Access Protocol	SNMP
Community String	<*your own*>

Settings for MySQL Server JBDC Access Credentials for Performance Monitoring

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your MySQL Server over JDBC for performance monitoring:

Setting	Value
Name	MySQL-Performance-Monitoring
Device Type	Oracle MySQL
Access Protocol	JBDC
Used For	Performance Monitoring
Pull Interval (minutes)	5
Port	3306
User Name	The administrative user for the database server
Password	The password associated with the administrative user

Settings for MySQL Server JBDC Access Credentials for Database Auditing

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your MySQL Server over JDBC for database auditing:

Setting	Value
Name	MySQL-Audit
Device Type	Oracle MySQL
Access Protocol	JBDC
Used For	Audit
Pull Interval (minutes)	5
Port	3306
Database Name	<*database name*> (MySQL)
Audit Table	dba_audit_trail
User Name	The administrative user for the database server
Password	The password associated with the administrative user

Settings for MySQL Server JBDC Access Credentials for Synthetic Transaction Monitoring, Snort Audit, McAfee VulnMgr

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your MySQL Server over JDBC for Synthetic Transaction Monitoring, Snort Audit, or McAfee VulnMgr:

Setting	Value
Name	*<name>*
Device Type	Oracle MySQL
Access Protocol	JBDC
Used For	Synthetic Transaction Monitoring, Snort Audit, or McAfee VulnMgr
Pull Interval (minutes)	5
Port	3306
Database Name	*<database name>*
User Name	The administrative user for the database server
Password	The password associated with the administrative user

Sample Events

- System Level Performance Metrics
- Table Space Performance Metrics
- Logon/Logoff Events
- Database CREATE/DELETE/MODIFY Events
- Table CREATE/DELETE/MODIFY Events

System Level Performance Metrics

```
<134>Apr 21 19:06:07 10.1.2.8 java: [PH_DEV_MON_PERF_MYSQLDB]: [eventSeverity]=PHL_INFO,
[hostIpAddr]=172.16.22.227, [hostName]=MYSQL, [appGroupName]=MySQL Database
Server, [appVersion]=MySQL 5.6.11, [charSetting]=utf8, [dbConnections]=24, [dbComUpdate]=0,
[dbComSelect]=1, [dbComInsert]=0,
[dbComDelete]=0, [dbCreatedTmpTables]=0, [dbSlowQueries]=0, [dbQcacheHits]=0,
[dbQcacheQueriesinCache]=0,
[dbQuestions]=7, [dbThreadsConnected]=1, [dbThreadsRunning]=1
```

Table Space Performance Metrics

```
<134>Apr 29 10:06:07 172.16.22.227 java: [PH_DEV_MON_PERF_MYSQLDB_TABLESPACE]:
[eventSeverity]=PHL_INFO, [appGroupName]=MySQL Database Server,
[instanceName]=mysql, [tablespaceName]=general_log, [tablespaceType]=PERMANENT,
[tablespaceUsage]=0.01, [tablespaceFreeSpace]=4193886,
[dbEngine]=MyISAM, [tableVersion]=10, [tableRowFormat]=dynamic, [tableRows]=124,
[tableAvgRowLength]=80, [tableIndexLength]=1024,
[tableCreateTime]=2013-04-29 15:12:30, [tableUpdateTime]=2013-04-29 12:35:46,
[tableCollation]=utf8_general_ci
```

Logon/Logoff Events

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_ Logon_Success]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [logonTime]=2013-04-29 15:14:54, [logoffTime]=,
[actionName]=Connect, [msg]=admin@172.16.22.227 on

<134>Apr 10 14:29:22 abc-desktop java: [MYSQL_Logoff]:[eventSeverity]=PHL_INFO,
[eventTime]=2013-04-10 14:29:22, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [logonTime]=, [logoffTime]=2014-04-10 14:29:22,
[actionName]=quit, [msg]=

<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_ Logon_Fail]: [eventSeverity]=PHL_WARN,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
 [srcIp]=172.16.22.227, [user]=admin, [logonTime]=2013-04-29 15:14:54, [logoffTime]=,
[actionName]=Connect,
[msg]=Access denied for user 'admin'@'172.16.22.227' (using password: YES)
```

Database CREATE/DELETE/MODIFY Events

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Create_database]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=create database sliutest

<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Drop_database]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=drop database sliutest
```

Table CREATE/DELETE/MODIFY Events

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Create_table]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=CREATE TABLE tutorials_tbl(
  tutorial_id INT NOT NULL AUTO_INCREMENT,
tutorial_title VARCHAR(100) NOT NULL,     tutorial_author VARCHAR(40) NOT NULL,
submission_date DATE,     PRIMARY KEY ( tutorial_id )    )

<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Delete_table]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=DELETE FROM tutorials_tbl
WHERE tutorial_id=2NOT NULL,
tutorial_author VARCHAR(40) NOT NULL,     submission_date DATE,     PRIMARY KEY ( tutorial_
id )

<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Insert_table]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=INSERT INTO tutorials_tbl
  (tutorial_title, tutorial_author, submission_date)
    VALUES      ("Learn Java", "John Smith", NOW())

<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_Drop_table]: [eventSeverity]=PHL_INFO,
[eventTime]=2013-04-29 15:14:54, [rptIp]=172.16.22.227,
[srcIp]=172.16.22.227, [user]=admin, [actionName]=Query, [msg]=DROP table sliutable
```

Oracle Database Server

Supported Versions

- Oracle Database 10g
- Oracle Database 11g
- Oracle Database 12c

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
JDBC		**Generic database information**: version, Character Setting, Archive Enabled, Listener Status, Instance Status, Last backup date,	
JDBC		**Database performance metrics:** Buffer cache hit ratio, Row cache hit ratio, Library cache hit ratio, Shared pool free ratio, Wait time ratio, Memory Sorts ratio, Host CPU Util ratio, CPU Time ratio, Disk Read/Write rates (operations and MBps), Network I/O Rate, Enqueue Deadlock rate, Database Request rate, User Transaction rate, User count, Logged on user count, Session Count, System table space usage, User table space usage, Temp table space usage, Last backup date, Days since last backup **Table space performance metrics**: Table space name, table space type, table space usage, table space free space, table space next extent	Performance Monitoring
Syslog		**Listener log, Alert log, Audit Log**	

Protocol	Information discovered	Metrics collected	Used for
JDBC	None	**Database audit trail:** Successful and failed database logon, Various database operation audit trail including CREATE/ALTER/DROP/TRUNCATE operations on tables, table spaces, databases, clusters, users, roles, views, table indices, triggers etc.	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "oracle database" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "oracle database" in the main content panel **Search...** field to see the rules associated with this application or device.

Reports

In **RESOURCES > Reports**, search for "oracle database" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- SNMP
- JDBC for Database Performance Monitoring - Oracle Database Server
- JDBC for Database Auditing - Oracle Database Server
- Configuring Listener Log and Error Log via SNARE - Oracle Side

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

JDBC for Database Performance Monitoring - Oracle Database Server

To configure your Oracle Database Server for performance monitoring by FortiSIEM, you must create a read-only user who has select permissions for the database. This is the user you will use to create the access credentials for FortiSIEM to communicate with your database server.

1. Open the SQLPlus application.
2. Log in with a system-level account.

3. Connect to your instance as sysdba.

   ```
   SQL> conn / as sysdba;
   Connected.
   ```

4. Create a non-admin user account. (**Note:** If you already created the `phoenix_agent` user, you can skip this step.)

   ```
   SQL> create user phoenix_agent identified by
   "accelops";
   User created.
   ```

5. Assign permissions to the user.
   ```
   grant select on dba_objects to phoenix_agent;
   grant select on dba_tablespace_usage_metrics to phoenix_agent;
   grant select on dba_tablespaces to phoenix_agent;
   grant select on nls_database_parameters to phoenix_agent;
   grant select on v_$backup_set to phoenix_agent;
   grant select on v_$instance to phoenix_agent;
   grant select on v_$parameter to phoenix_agent;
   grant select on v_$session to phoenix_agent;
   grant select on v_$sql to phoenix_agent;
   grant select on v_$sysmetric to phoenix_agent;
   grant select on v_$version to phoenix_agent;
   grant select on gv_$session to phoenix_agent;
   grant select on gv_$service_stats to phoenix_agent;
   ```
6. Verily that the permissions were successfully assigned to the user.
   ```
   select count(*) from dba_objects;
   select count(*) from dba_tablespace_usage_metrics;
   select count(*) from dba_tablespaces;
   select count(*) from gv$service_stats;
   select count(*) from nls_database_parameters;
   select count(*) from v$backup_set order by start_time desc;
   select count(*) from v$instance;
   select count(*) from v$parameter;
   select count(*) from v$session;
   select count(*) from v$sql;
   select count(*) from v$sysmetric;
   select count(*) from v$version;
   ```

JDBC for Database Auditing - Oracle Database Server

Required Environmental Variables

Make sure that these environment variables are set

- `ORACLE_HOME= C:\app\Administrator\product\11.2.0\dbhome_1`
- `ORACLE_BASE= C:\app\Administrator`

1. Create audit trail views by executing `cataaudit.sql` as the `sysdb` user.

   ```
   Linux:
   su- oracle
    sqlplus /nolog
    conn / as sysdba;
    @$ORACLE_HOME/rdbms/admin/cataudit.sql;
   quit

   Windows:
   ```

```
sqlplus /nolog
conn / as sysdba;
@%ORACLE_HOME%/rdbms/admin/cataudit.sql;
quit
```

2. Enable auditing by modifying the Oracle instance initialization file `init<SID>.ora`.
   This is typically located in `$ORACLE_BASE/admin/<SID>/pfile` where `DIS` is the Oracle instance

   ```
   AUDIT_TRAIL = DB
   or
   AUDIT_TRAIL = true
   ```

3. Restart the database.

   ```
   su - oracle
    sqlplus /nolog
    conn / as sysdba;
    shutdown immediate;
    startup;
    quit
   ```

4. Create a user account and grant select privileges to that user.

   ```
   su - oracle
    sqlplus /nolog
    conn / as sysdba
    Create user phoenix_agent identified by "phoenix_agent_pwd"   (NOTE: please correct
   this set -- above steps showed that we created phoenix_agent already, just add the grant
   steps and utilize the "accelops" password;
    Grant connect to phoenix_agent;
    Grant select on dba_audit_trail to phoenix_agent;
    Grant select on v_$session to phoenix_agent;
   ```

5. Turn on auditing.

   ```
   su - oracle
   sqlplus /nolog
   conn / as sysdba;
   audit session;
   quit;
   ```

6. Fetch the audit data to make sure the configuration was successful.

   ```
   su - oracle;
    sqlplus phoenix_agent/phoenix_agent_pwd;
    select count (*) from dba_audit_trail;
   ```

   You should see the count changing after logging on a few times.

Configuring Listener Log and Error Log via SNARE - Oracle Side

1. Install and configure Epilog application to send syslog to FortiSIEM
   a. Download Epilog from snare, information to download here, and install it on your Windows Server.
   b. Launch Epilog from Start→All Programs→InterSect Alliance→Epilog for windows
   c. Configure Epilog application as follows
      i. Select Log Configuration on left hand panel, click Add button to add Oracle Listener log file to be sent to FortiSIEM. **Also make sure the Log Type is OracleListenerLog**.

ii. Click Add button to add Oracle Alert log file to be sent to FortiSIEM. **Also make sure the Log Type is OracleAlertLog**.
iii. After adding both the files, SNARE Log Configuration will show both the files included as follows
iv. Select Network Configuration on left hand panel. On the right, set the destination address to that of FortiSIEM server, port to 514 and make sure that syslog header is enabled. Then click Change Configuration button.
v. Click the "Apply the latest audit configuration" link on the left hand side to apply the changes to Epilog applications. DHCP logs will now sent to FortiSIEM in real time.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Settings for Oracle Database Server JDBC Access Credentials for Performance Monitoring

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Settings for Oracle Database Server JDBC Access Credentials for Performance Monitoring

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your Oracle database server over JDBC:

Setting	Value
Name	phoenix_agent_accelops
Device Type	Oracle Database Server
Access Protocol	JDBC
Used For	Performance Monitoring
Pull Interval (minutes)	5

Setting	Value
Port	1521
Instance Name	orcl2
User Name	The user you created for performance monitoring
Password	The password associated with the user

Sample Events

- System Level Database Performance Metrics
- Table Space Performance Metrics
- Oracle Audit Trail (FortiSIEM Generated Events)
- Oracle Audit Log
- Oracle Listener Log
- Oracle Alert Log

System Level Database Performance Metrics

```
[PH_DEV_MON_PERF_ORADB]:[eventSeverity]=PHL_INFO, [hostIpAddr]=10.1.2.8, [hostName]=Host-
10.1.2.8, [appGroupName]=Oracle Database Server,
[appVersion]=Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - Production,
[instanceName]=orcl, [instanceStatus]=OPEN, [charSetting]=ZHS16GBK, [archiveEnabled]=FALSE,
 [lastBackupDate]=1325566287, [listenerStatus]=OPEN,[dbBufferCacheHitRatio]=100,
[dbMemorySortsRatio]=100,[dbUserTransactionPerSec]=0.13,[dbPhysicalReadsPerSec]=0,
[dbPhysicalWritesPerSec]=0.48,[dbHostCpuUtilRatio]=0,[dbNetworkKBytesPerSec]=0.58,
[dbEnqueueDeadlocksPerSec]=0,[dbCurrentLogonsCount]=32,[dbWaitTimeRatio]=7.13,
[dbCpuTimeRatio]=92.87,
[dbRowCacheHitRatio]=100,[dbLibraryCacheHitRatio]=99.91,[dbSharedPoolFreeRatio]=18.55,
[dbSessionCount]=40,[dbIOKBytesPerSec]=33.26,[dbRequestsPerSec]=3.24,
[dbSystemTablespaceUsage]= 2.88,[dbTempTablespaceUsage]= 0,[dbUsersTablespaceUsage]= 0.01,
[dbUserCount]= 2,[dbInvalidObjectCount]= 4
```

Table Space Performance Metrics

```
[PH_DEV_MON_PERF_ORADB_TABLESPACE]:[eventSeverity]=PHL_INFO, [appGroupName]=Oracle Database
Server, [instanceName]=orcl, [tablespaceName]=UNDOTBS1, [tablespaceType]=UNDO,
[tablespaceUsage]=0.01, [tablespaceFreeSpace]=4193886, [tablespaceNextExtent]=0

[PH_DEV_MON_PERF_ORADB_TABLESPACE]:[eventSeverity]=PHL_INFO, [appGroupName]=Oracle Database
Server, [instanceName]=orcl, [tablespaceName]=USERS, [tablespaceType]=PERMANENT,
[tablespaceUsage]=0.01, [tablespaceFreeSpace]=4193774, [tablespaceNextExtent]=0
```

Oracle Audit Trail (FortiSIEM Generated Events)

```
<134>Apr 10 12:51:42 abc-desktop java: [ORADB_PH_Logoff]:[eventSeverity]=PHL_INFO,
[retCode]=0, [eventTime]=2009-04-10 14:29:22:111420, [rptIp]=172.16.10.40, [srcIp]=QA-V-
CtOS-ora.abc.net, [user]=DBSNMP, [logonTime]=2009-04-10 14:29:22:111420, [logoffTime]=2009-
04-10 14:29:22, [privUsed]=CREATE_SESSION,
```

Oracle Audit Log

```
<172>Oracle Audit[25487]: LENGTH : '153' ACTION :[004] 'bjn' DATABASE USER:[9] 'user'
PRIVILEGE :[4] 'NONE' CLIENT USER:[9] 'user' CLIENT TERMINAL:[14] 'terminal' STATUS:[1] '0']

<172>Oracle Audit[6561]: LENGTH : '158' ACTION :[6] 'COMMIT' DATABASE USER:[8] 'user'
PRIVILEGE :[6] 'SYSDBA' CLIENT USER:[6] 'user' CLIENT TERMINAL:[0] '' STATUS:[1] '0' DBID:
[9] '200958341'

<172>Oracle Audit[28061]: LENGTH: 265 SESSIONID:[9] 118110747 ENTRYID:[5] 14188 STATEMENT:
[5] 28375 USERID:[8] user ACTION:[3] 100 RETURNCODE:[1] 0 COMMENT$TEXT:[99] Authenticated
by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=10.90.217.247)(PORT=4566))
PRIV$USED:[1] 5
```

Oracle Listener Log

```
<46>Dec 13 06:07:08 WIN03R2E-110929    OracleListenerLog    0    12-OCT-2011 16:17:52 *
(CONNECT_DATA=(CID=(PROGRAM=)(HOST=)(USER=Administrator))(COMMAND=status)(ARGUMENTS=64)
(SERVICE=LISTENER)(VERSION=185599744)) * status * 0
```

Oracle Alert Log

```
<46>Dec 13 06:07:08 WIN03R2E-110929 OracleAlertLog    0    ORA-00312: online log 3 thread 1:
'C:\APP\ADMINISTRATOR\ORADATA\ORCL\REDO03.LOG'
```

DHCP and DNS Server

FortiSIEM supports these DHCP and DNS servers for discovery and monitoring.

- Infoblox DNS/DHCP
- ISC BIND DNS
- Linux DHCP
- Microsoft DHCP (2003, 2008)
- Microsoft DNS (2003, 2008)

Infoblox DNS/DHCP

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host Name, Hardware model, Serial number, Network Interfaces, Running processes, Installed software	System CPU utilization, Memory utilization, Disk usage, Disk I/O	Performance Monitoring
SNMP		Process level CPU utilization, Memory utilization	
SNMP		**Zone Transfer metrics**: For each zone: DNS Responses Sent, Failed DNS Queries, DNS Referrals, Non-existent DNS Record Queries, DNS Non-existent Domain Queries, Recursive DNS Query Received **DNS Cluster Replication metrics**: DNS Replication Queue Status, Sent Queue From Master, Last Sent Time From Master, Sent Queue To Master, Last Sent Time To Master **DNS Performance metrics**: NonAuth DNS Query Count, NonAuth Avg DNS Latency, Auth DNS Query Count, Auth Avg DNS Latency, Invalid DNS Port Response, Invalid DNS TXID Response **DHCP Performance metrics**: Discovers/sec, Requests/Sec, Releases/Sec, Offers/sec, Acks/sec, Nacks/sec, Declines/sec, Informs/sec **DDNS Update metrics**: DDNS Update Success, DDNS Update Fail, DDNS Update Reject, DDNS Prereq Update Reject, DDNS Update Latency, DDNS Update Timeout **DHCP subnet usage metrics**: For each DHCP Subnet (addr, mask) - percent used	Security Monitoring and compliance
SNMP		Hardware status	Availability monitoring
SNMP Trap		Hardware failures, Software failures	Availability monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "infoblox" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "infoblox" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

ISC BIND DNS

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials
- Sample BIND DNS Logs

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
Syslog	Application type	**DNS name resolution activity**: DNS Query Success and Failure by type	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "isc bind" to see the event types associated with this device.

Configuration

- SNMP
- Syslog

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

Configure the ISC BIND DNS Server to Send Syslog

1. Edit `named.conf` and add a new line: `include /var/named/conf/logging.conf;`.
2. Edit the `/var/named/conf/logging.conf` file, and in the `channel queries_file { }` section add `syslog local3;`
3. Restart BIND by issuing `/etc/init.d/named restart`.

Configure Syslog to Send to FortiSIEM

1. Edit `syslog.conf` and add a new line: `Local7.* @<IP address of the FortiSIEM server>.`
2. Restart the syslog daemon by issuing `/etc/init.d/syslog restart`.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Sample BIND DNS Logs

```
<158>Jan 28 20:41:46 100.1.1.1 named[3135]: 28-Jan-2010 20:40:28.809 client
192.168.29.18#34065: query: www.google.com IN A +
```

Linux DHCP

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
Syslog	Application type	**DHCP address release/renew events** that are used by FortiSIEM for Identity and location: attributes include IP Address, MAC address, Host Name	Security and compliance (associate machines to IP addresses)

Event Types

In **ADMIN > Device Support > Event Types**, search for "linux dhcp" to see the event types associated with this device.

Configuration

- SNMP
- Syslog
- Sample Syslog

SNMP

1. Make sure that snmp libraries are installed.
   FortiSIEM has been tested to work with net-snmp libraries.
2. Log in to your device with administrator credentials.
3. Modify the `/etc/snmp/snmpd.conf` file:
   a. Define the community string for FortiSIEM usage and permit snmp access from FortiSIEM IP.
   b. Allow FortiSIEM to (read-only) view the mib-2 tree.
   c. Open up the entire tree for read-only view.
4. Restart the snmpd deamon by issuing `/etc/init.d/snmpd restart`.
5. Add the snmpd daemon to start from boot by issuing `chkconfig snmpd on`.
6. Make sure that snmpd is running.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

Configure Linux DHCP to Forward Logs to Syslog Daemon

1. Edit `dhcpd.conf` and insert the line `log-facility local7;`.
2. Restart dhcpd by issuing `/etc/init.d/dhcpd restart`.

Configure Syslog to Forward to FortiSIEM

1. Edit `syslog.conf` and add a new line: `Local7.* @<IP address of FortiSIEM server>`.
2. Restart syslog daemon by issuing `/etc/init.d/syslog restart`.

Sample Syslog

```
<13>Aug 26 19:28:11 DNS-Pri dhcpd: DHCPREQUEST for 172.16.10.200 (172.16.10.8) from
00:50:56:88:4e:17 (26L2233B1-02)
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Microsoft DHCP

- Supported OS
- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Controls

Supported OS

- Windows 2003
- Windows 2008 and 2008 R2
- Windows 2012 and 2012 R2
- Windows 2016
- Windows 2019

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Process details	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Process details, process to service mappings	**Process level metrics (Win32_Process, Win32_PerfRawData_PerfProc_Process)**: uptime, CPU utilization, Memory utilization, Read I/O, Write I/O **DHCP metrics (Win32_PerfFormattedData_DHCPServer_DHCPServer)**: DHCP request rate, release rate, decline rate, Duplicate Drop rate, Packet Rate, Active Queue length, DHCP response time, Conflict queue length	Performance Monitoring
Windows Agent	Application type	**DHCP address release/renew events** that are used by FortiSIEM for Identity and location: attributes include IP Address, MAC address, Host Name	Security and compliance (associate machines to IP addresses)

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft dhcp" to see the event types associated with this device.

Configuration

- SNMP
- WMI
- FortiSIEM Windows Agent

SNMP

See SNMP Configurations in the *Microsoft Windows Server Configuration* section.

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring DHCP for FortiSIEM Windows Agent, see Configuring Windows DHCP in the *Windows Agent Installation Guide*.

Settings for Access Controls

See Setting Access Credentials in the *Microsoft Windows Server Configuration* section.

Microsoft DNS

- Supported OS
- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials

Supported OS

- Windows 2003
- Windows 2008 and 2008 R2
- Windows 2012 and 2012 R2
- Windows 2016
- Windows 2019

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU utilization, Memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics (Win32_Process, Win32_PerfRawData_PerfProc_Process)**: uptime, CPU utilization, Memory utilization, Read I/O, Write I/O **DNS metrics (Win32_PerfFormattedData_DNS_DNS)**: DNS requests received, DNS responses sent, WINS requests received, WINS responses sent, Recursive DNS queries received, Recursive DNS queries failed, Recursive DNS queries timeout, Dynamic DNS updates received, Dynamic DNS updates failed, Dynamic DNS updates timeout, Secure DNS update received, Secure DNS update failed, Full DNS Zone Transfer requests sent, Full DNS Zone Transfer requests received, Incremental DNS Zone Transfer requests sent, ncremental DNS Zone Transfer requests received	Performance Monitoring
Windows Agent	Application type	**DNS name resolution activity**: DNS Query Success and Failure by type	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft dns" to see the event types associated with this device.

Configuration

- SNMP
- WMI
- FortiSIEM Windows Agent

SNMP

See SNMP Configurations in the *Microsoft Windows Server Configuration* section.

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring DNS for FortiSIEM Windows Agent, see Configuring Windows DNS in the *Windows Agent 6.3.2 Installation Guide*.

Microsoft recommends that customers enable DNS Analytical logs only to debug DNS traffic or to troubleshoot DNS server issues. Enabling DNS Analytical logs can cause system performance issues (see Microsoft Logging and Diagnostics).

Settings for Access Credentials

See Setting Access Credentials in the *Microsoft Windows Server Configuration* section.

Directory Server

FortiSIEM supports this directory server for discovery and monitoring.

- Microsoft Active Directory

Microsoft Active Directory

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
LDAP	User details, Password age		Security Monitoring, User meta data for log
WMI		Win32_PerfRawData_NTDS_NTDS class: Directory Search Rate, Read Rate, Write Rate, Browse Rate, LDAP search rate, LDAP Bind Rate, New LDAP Connection Rate, Successful LDAP Bind Rate, LDAP Active Threads, LDAP Bind Time, LDAP Client Sessions	Performance Monitoring
WMI		"dcdiag -e" command output - detect successful and failed domain controller diagnostic tests	Domain Controller Replication status
WMI		"repadmin /replsummary" command output - detect replication statistics	Domain Controller Replication status

Event Types

- PH_DISCOV_ADS_ACCOUNT_TO_EXPIRE (Active Directory account to expire in 2 weeks)
- PH_DISCOV_ADS_ACCT_DISABLED (Accounts Disabled)
- PH_DISCOV_ADS_DORMANT_ACCT (Dormant User Accounts - not log on in last 30 days)
- PH_DISCOV_ADS_PASSWORD_NEVER_EXPIRES (Active Directory user password never expires)
- PH_DISCOV_ADS_PASSWORD_NOT_REQD (Active Directory user password not required)
- PH_DISCOV_ADS_PASSWORD_STALE (Active Directory user password stale - more than 90 days)
- PH_DISCOV_ADS_PASSWORD_TO_EXPIRE (Active Directory user password to expire in 2 weeks)

- PH_DEV_MON_DCDIAG (output of "dcdiag -e" command)

  ```
  [PH_DEV_MON_DCDIAG]:[hostIpAddr]=10.1.20.59,[hostName]=WIN-IGO8O8M5JVT,[errReason]="",
  [testResult]="passed",[testSubject]="WIN-IGO8O8M5JVT",[testName]="NCSecDesc"
  ```

- PH_DEV_MON_SRC_AD_REPL_STAT (output of "repadmin /replsummary" command)

  ```
  [PH_DEV_MON_SRC_AD_REPL_STAT]:[hostIpAddr]=10.1.20.59,[hostName]=WIN-IGO8O8M5JVT,
  [largestReplDelta]=">60 days",[failureCount]=0.00,[count]=5.00,[failurePct]=0.00,
  [srcName]="WIN-IGO8O8M5JVT",[errReason]=""
  ```

- PH_DEV_MON_DST_AD_REPL_STAT (output of "repadmin /replsummary" command)

  ```
   [PH_DEV_MON_DST_AD_REPL_STAT]:[hostIpAddr]=10.1.20.59,[hostName]=WIN-IGO8O8M5JVT,
  [largestReplDelta]=">60 days",[failureCount]=0.00,[count]=5.00,[failurePct]=0.00,
  [destName]="WIN-IGO8O8M5JVT",[errReason]=""
  ```

Rules

- Failed Windows DC Diagnostic Test

Reports

- Successful Windows Domain Controller Diagnostic Tests
- Failed Windows Domain Controller Diagnostic Tests
- Source Domain Controller Replication Status
- Destination Domain Controller Replication Status

Configuration

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

Active Directory User Discovery

If you want to add Active Directory users to FortiSIEM, follow these steps in the FortiSIEM UI.

1. Add the login credentials for Active Directory server and associate them to an IP range.
2. Discover the Active Directory server.

If the Active Directory server is discovered successfully, then all of the users and their properties will be added to FortiSIEM.

After the users have been added to FortiSIEM, you can re-run discovery to get new changes from Active Directory. You cannot make changes in FortiSIEM as this will inevitably make FortiSIEM out of synch with Active Directory.

Since Active Directory can contain many users, it is possible to choose a sub-tree by specifying a base DN (see below).

Adding Active Directory Login Credentials to FortiSIEM

1. Log in to your Supervisor UI.
2. Go to **ADMIN > Setup > Credentials**.
3. Click **New** to create an LDAP discovery credential by entering the following in the Access Method Definition dialog box:
   a. **Name**: a name for the credential.
   b. **Device Type**: select **Microsoft Windows**.
   c. **Access Protocol**:
      i. By default, **LDAP** servers listen on TCP port 389.
      ii. **LDAPS** (LDAP with SSL) defaults to port 636.
      iii. **LDAP** Start TLS defaults to port 389.
   d. **Used For**: select **Microsoft Active Directory**.
   e. Enter the root of the **LDAP** user tree that you want to discover. For example, `dc=`*`companyABC`*`,dc=com` or `ou=Org1,dc=`*`companyABC`*`,dc=com`
   f. **NetBIOS/Domain**: enter the NetBIOS/Domain value.
   g. **User Name**: enter the user name for your LDAP directory.
      The user should be a member of the **Domain Users** group in Active Directory. See the Validating LDAP Credentials and Permissions for information on how to validate this membership.
   h. Enter and confirm the **Password** for your User.
   i. Click **Save**. Your LDAP credentials will be added to the list of credentials.
4. Under **Enter IP Range to Credential Associations**, click **Add**.
5. Select your **LDAP** credentials from the list of **Credentials**. Click **+** to add more.
6. Enter the **IP/IP Range** or **host name** for your Active Directory server.
7. Click **Save**. Your LDAP credentials will appear in the list of credential/IP address associations.
8. Click **Test > Test Connectivity** to make sure you can connect to the Active Directory server.

Discovering Users in FortiSIEM

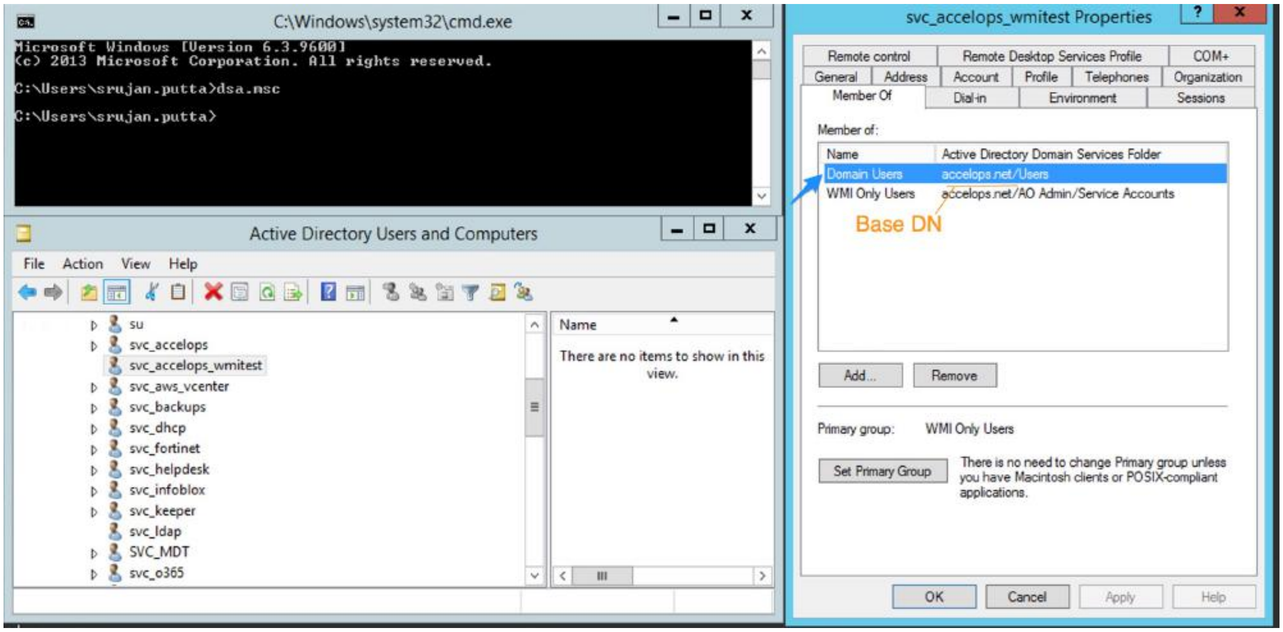
1. Go to **ADMIN > Setup > Discovery** and click **New**.
2. For **Name**, enter **Active Directory**.
3. For **Include**, enter the IP address or host name for your Active Directory server.
4. Click **Save**. Active Directory will be added to the list of discoverable devices.
5. Select the **Active Directory** device and click **Discover**.
6. After discovery completes, go to **CMDB > Users** to view the discovered users. You may need to click the **Refresh** icon to load the user tree hierarchy.

To get user updates in Active Directory, simply re-run discovery.

Validating LDAP Credentials and Permissions

1. Log in to your Active Directory server.
2. Open the Active Directory console from the command prompt and execute the `dsa.msc` command.

3. From the Active Directory console, select the User that added in FortiSIEM Supervisor.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\srujan.putta>dsa.msc

C:\Users\srujan.putta>
```

There are no items to show in this view.

Member of:

Name	Active Directory Domain Services Folder
Domain Users	accelops.net/Users
WMI Only Users	accelops.net/AO Admin/Service Accounts

Primary group: WMI Only Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

4. Right click the selected User and check **Properties**.
5. The User should be a member of **Domain Users**.
6. On FortiSIEM **Base DN** should match, example: `DC=accelops,DC=net`.

Mapping Active Directory User Attributes to FortiSIEM User Attributes

The following table shows how user attributes in Microsoft Active Directory are shown in the FortiSIEM UI. To find Active Directory user attributes, take the following steps:

1. Log in to Active Directory.
2. Go to Active Directory Users and Computers.
3. Click **View** > **Enable Advanced Features**.
4. Find a user, and take the following steps:
   a. Double click user.
   b. Click Attribute Editor.
   You will see a set of attributes and the values they are set to.

In FortiSIEM, user details can be found in **CMDB** > **Users**. First, click the tree node on the left that you have discovered, then locate the user in the right pane. Attributes are displayed on the main page and under Summary, Contact, and Member Of.

Microsoft Active Directory User Attribute	FortiSIEM User Attribute
sAMAccoutName	User Name
name	Full Name
userPrincipalName	<Not shown>

Microsoft Active Directory User Attribute	FortiSIEM User Attribute
mail	Email
telephoneNumber	Work Phone
mobile	Mobile Phone
title	Job Title
company	Company
department	<Not shown>
employeeID	Employee ID
manager	Manager
l	<Not shown>
postalCode	ZIP
streetAddress	Address
homePostalAddress	<Not shown>
c	City
st	State
co	Country
memberOf	Member Of

Document Management Server

FortiSIEM supports this document management server for discovery and monitoring.

- Microsoft SharePoint

Microsoft SharePoint

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
LOGbinder Agent		SharePoint logs - Audit trail integrity, Access control changes, Document updates, List updates, Container object updates, Object changes, Object Import/Exports, Document views, Information Management Policy changes	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "sharepoint" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "sharepoint" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

Microsoft SharePoint logs are supported via LOGbinder SP agent from Monterey Technology group. The agent must be installed on the SharePoint server. **Configure the agent to write logs to Windows Security log**. FortiSIEM simply reads the logs from windows security logs via WMI and categorizes the SharePoint specific events and parses SharePoint specific attributes.

Installing and Configuring LOGbinder SP Agent

- LOGbinder Install Web Link
- LOGbinder Configuration Web Link - Remember to configure LOGbinder SP agent to write to Windows security log.
- LOGbinder SP Getting Started Document - Remember to configure LOGbinder SP agent to write to Windows security log.

Healthcare IT

FortiSIEM supports the discovery and monitoring of these healthcare applications.

- Epic EMR/EHR System

Epic EMR/EHR System

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Authentication Query, Client login Query	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Epic-SecuritySIEM" to see the event types associated with this device. There are two events that are parsed:

- `Epic-SecuritySIEM-AUTHENTICATION-Query`
- `Epic-SecuritySIEM-LOGIN-Query`

Rules

No specific rules are written for Epic-SecuritySIEM.

Reports

No specific reports are written for Epic-SecuritySIEM.

Configuration

Configure the Epic-SecuritySIEM system to send logs to FortiSIEM in the supported format (see Sample Events).

Settings for Access Credentials

None required.

Sample Events

```
Oct 19 05:32:16 10.25.8.111 CEF:0|Epic|Security-SIEM|8.3.0|LOGIN|LOGIN|4|cnt=1
suser=3227^DOE, JOHN L^JOHN-DOE shost=PRD workstationID=WS7946 act=Query
end=Oct 19 00:30:00 flag=^^Workflow Logging CLIENTNAME=dom1/WS7946
DEP=100000010^RMC ICU MAIN IP=10.25.6.59/10.170.10.66 LOGINLDAPID=JOHN-DOE
LOGINREASON= OSUSR=WS7946 ROLE=MODEL IP NURSE SOURCE=1-Hyperspace
USERJOB=304401^RMC INPATIENT NURSE TEMPLATE#011

Oct 19 05:32:16 10.25.8.111 CEF:0|Epic|Security-
     SIEM|8.3.0|AUTHENTICATION|AUTHENTICATION|4|cnt=1
suser=3055^DOE, JOHN^JOHN-DOE shost=PRD workstationID=WS7610 act=Query end=Oct 19 00:30:00
flag=Access History^^Workflow Logging LOGINCONTEXT=0-Login
LOGINDEVICE=10001-ImprivataAuthMultiApp LOGINLDAPID=JOHN-DOE LOGINREVAL= 011
```

Mail Server

FortiSIEM supports this mail server for discovery and monitoring.

- Microsoft Exchange

Microsoft Exchange

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Logs

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	Process level CPU and memory utilization for the various exchange server processes	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec for the various exchange server processes	Performance Monitoring
		Exchange performance metrics (: VM Largest Block size, VM Large Free Block Size, VM Total Free Blocks, RPC Requests, RPC Request Peak, RPC Average Latency, RPC Operations/sec, User count, Active user Count, Peak User Count, Active Connection Count, Max Connection Count **Exchange error metrics** (obtained from Win32_PerfRawData_MSExchangeIS_MSExchangeIS WMI class): RPC Success, RPC Failed, RPC Denied, RPC Failed - Server Busy, RPC Failed - Server Unavailable, Foreground RPC Failed, Backgorund RPC Failed **Exchange mailbox metrics** (obtained from Win32_PerfRawData_MSExchangeIS_MSExchangeISMailbox and Win32_PerfRawData_MSExchangeIS_MSExchangeISPublic WMI classes): Per Mailbox: Send Queue, Receive Queue, Sent Message, Submitted Message, Delivered Message, Active User, Peak User	
		Exchange SMTP metrics (obtained from Win32_PerfRawData_SMTPSVC_SMTPServer WMI class): Categorization Queue, Local Queue, Remote Queue, Inbound Connections, Outbound Connections, Sent Bytes/sec, Received Bytes/sec, Retry Count, Local Retry Queue, Remote Retry Queue	

Protocol	Information discovered	Metrics collected	Used for

		Exchange ESE Database (Win32_PerfFormattedData_ESE_MSExchangeDatabase):
		Exchange Database Instances (Win32_PerfFormattedData_ESE_MSExchangeDatabaseInstances):	

		Exchange Mail Submission Metrics (Win32_PerfFormattedData_MSExchangeMailSubmission_MSExchangeMailSubmission):
		Exchange Replication Metrics (Win32_PerfFormattedData_MSExchangeReplication_MSExchangeReplication):
		Exchange Store Interface Metrics (Win32_PerfFormattedData_MSExchangeStoreInterface_MSExchangeStoreInterface):
		Exchange Transport Queue Metrics (Win32_PerfFormattedData_MSExchangeTransportQueues_MSExchangeTransportQueues):	

Windows Agent		Application Logs	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft exchange" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "microsoft exchange" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- SNMP
- WMI

SNMP

See SNMP Configurations in the *Microsoft Windows Server Configuration* section.

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

Settings for Access Credentials

See Setting Access Credentials in the *Microsoft Windows Server Configuration* section.

Sample Logs

```
2017-10-05T12:06:00Z SRV-EXCH33.sample.exa 192.0.2.105 AccelOps-WUA-UserFile-
ExchangeTrackLog [monitorStatus]="Success" [Locale]="en-US" [MachineGuid]="d78e4bd5-bc3f-
4950-bcdf-926947ee1db7" [timeZone]="+0300" [fileName]="C:\\Program
Files\\Microsoft\\Exchange
Server\\V15\\TransportRoles\\Logs\\MessageTracking\\MSGTRKMS2017100512-1.LOG" [msg]="2017-
10-05T12:05:56.564Z,fe80::ac4c:6f22:1c25:97d8%13,SRV-EXCH02,,SRV-
EXCH55.sample.exa,\"MDB:d72c63cf-290e-456e-86e5-85dedb1f56de, Mailbox:d7c8c446-c8a7-4248-
a17f-772d5273403d, Event:4419662,
MessageClass:IPM.Note.ProbeMessage.MBTSubmissionServiceHeartbeatProbe, CreationTime:2017-10-
05T12:05:56.267Z, ClientType:Monitoring,
SubmissionAssistant:MailboxTransportSubmissionEmailAssistant\",,STOREDRIVER,SUBMIT,,<e545b61
2256a4c34a678f78a6433fafd@sample.ult.bi>,0a21180c-5932-4c7e-3888-
08d50be96f34,HealthMailbox55aa22abbc9d4ss47edh9yk75k745h0z@sample.ult.bi,,,1,,,00000052-
0000-0000-0000-0000ea5a2141-
MBTSubmissionServiceHeartbeatProbe,HealthMailbox55aa22abbc9d4ss47edh9yk75k745h0z@sample.ult.
bi,,2017-10-05T12:05:56.267Z;LSRV=SRV-EXCH33.sample.exa:TOTAL-SUB=0.296|SA=0.078|MTSS=0.209
(MTSSD=0.209(MTSSDA=0.005|MTSSDC=0.005|SDSSO=0.161(SMSC=0.020|SMS=0.140)|X-MTSSDPL=0.004|X-
MTSSDSS=0.008|MTSSDSDS=0.001)),Originating,,,,S:ItemEntryId=00-00-00-00-ED-99-60-31-E3-76-
3C-4B-BE-FE-5B-27-F0-88-3D-0A-07-00-25-D5-0C-8E-46-5A-51-46-A4-18-7D-65-F7-DF-52-1C-00-00-
00-00-01-0B-00-00-25-D5-0C-8E-46-5A-51-46-A4-18-7D-65-F7-DF-52-1C-00-00-30-88-0D-FF-00-
00,Email,92e0d0ab-4670-41e9-d453-08d50be96f50,15.01.0845.034"
```

Management Server/Appliance

FortiSIEM supports these web servers for discovery and monitoring.

- Cisco Application Centric Infrastructure (ACI)
- Fortinet FortiInsight
- Fortinet FortiManager

Cisco Application Centric Infrastructure (ACI)

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- FortiSIEM Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Cisco APIC API (REST)		Overall Health, Tenant Health, Node Health, Cluster Health, Application Health, EPG health, Fault Record, Event record, Log Record, Configuration Change	Availability and Performance Monitoring

Event Types

Go to **ADMIN > Device Support > Event Types** and search for "Cisco_ACI".

Rules

Go to **RESOURCES > Rules** and search for "Cisco ACI" in the main content panel **Search...** field.

Reports

Go to **RESOURCES > Reports** and search for "Cisco ACI" in the main content panel **Search...** field.

Configuration

- Cisco ACI Configuration
- FortiSIEM Configuration

Cisco ACI Configuration

Please configure Cisco ACI Appliance so that FortiSIEM can access it via APIC API.

FortiSIEM Configuration

1. Go to **ADMIN > Setup > Credentials**.
2. In **Step 1: Enter Credentials**, click **New** and create a credential.

Settings	Description
Name	Enter a name for the credential.
Device Type	CISCO CISCO ACI
Access Protocol	Cisco APIC API
Pull Interval	5 minutes
Port	443
Password config	See Password Configuration
User Name	User name for device access
Password	Password for the various REST APIs
Description	Password for the various REST APIs

3. In **Step 2: Enter IP Range to Credential Associations** click **New** and create the association.
   a. **IP** - specify the IP address of the ACI Controller
   b. **Credential** - specify the Name as in 2a
4. **Test Connectivity** - Click the **Test** drop-down list, and select **Test Connectivity** with or without ping and make sure the test succeeds
5. Check **Pull Events**, located by navigating to **ADMIN > Setup > Pull Events**, to make sure that a event pulling entry is created

Sample Events

- Overall Health Event
- Tenant Health Event
- Nodes Health Event
- Cluster Health Event
- Application Health Event
- EPG Health Event
- Fault Record Event
- Event Record Event
- Log Record Event
- Configuration Change Event

Overall Health Event

```
[Cisco_ACI_Overall_Health]: {"attributes":
{"childAction":"","cnt":"29","dn":"topology/HDfabricOverallHealth5min0","healthAvg":"82","he
althMax":"89",
"healthMin":"0","healthSpct":"0","healthThr":"","healthTr":"1","index":"0","lastCollOffset":
"290","repIntvEnd":"2016-09-05T08:13:53.232+00:00","repIntvStart":"2016-09-
05T08:09:03.128+00:00","status":""}}
```

Tenant Health Event

```
[Cisco_ACI_Tenant_Health]: {"attributes":{"childAction":"","descr":"","dn":"uni/tn-
CliQr","lcOwn":"local","modTs":"2016-09-05T07:56:27.164+00:00","monPolDn":"uni/tn-
common/monepg-
default","name":"CliQr","ownerKey":"","ownerTag":"","status":"","uid":"15374"},"children":
[{"healthInst":{"attributes":
{"childAction":"","chng":"0","cur":"100","maxSev":"cleared","prev":"100","rn":"health","stat
us":"",

"twScore":"100","updTs":"2016-09-05T08:27:03.584+00:00"}}}]
```

Nodes Health Event

```
[Cisco_ACI_Node_Health]: {"attributes":
{"address":"10.0.208.95","childAction":"","configIssues":"","currentTime":"2016-09-
05T08:15:51.794+00:00","dn":"topology/pod-1/node-
101/sys","fabricId":"1","fabricMAC":"00:22:BD:F8:19:FF","id":"101","inbMgmtAddr":"0.0.0.0",

"inbMgmtAddr6":"0.0.0.0","lcOwn":"local","modTs":"2016-09-05T07:57:29.435+00:00",

"mode":"unspecified","monPolDn":"uni/fabric/monfab-
default","name":"Leaf1","oobMgmtAddr":"0.0.0.0","oobMgmtAddr6":"0.0.0.0","podId":"1","role"

:"leaf","serial":"TEP-1-101","state":"in-
service","status":"","systemUpTime":"00:00:27:05.000"},"children":[{"healthInst":
{"attributes":{"childAction":"","chng":"-
10","cur":"90","maxSev":"cleared","prev":"100","rn":"health","status":"","twScore":"90","upd
Ts":"2016-09-05T07:50:08.415+00:00"}}}]
```

Cluster Health Event

```
[Cisco_ACI_Cluster_Health]: {"attributes":{"addr":"10.0.0.1","adminSt":"in-
service","chassis":"10220833-ea00-3bb3-93b2-
ef1e7e645889","childAction":"","cntrlSbstState":"approved","dn":"topology/pod-1/node-
1/av/node-1","health":"fully-fit","id":"1","lcOwn":"local","mbSn":"TEP-1-1","modTs":"2016-
09-05T08:00:46.797+00:00","monPolDn":"","mutnTs":"2016-09-
05T07:50:19.570+00:00","name":"","nodeName":"apic1","operSt":"available","status":"","uid":"
0"}
```

Application Health Event

```
[Cisco_ACI_Application_Health]: {"attributes":{"childAction":"","descr":"","dn":"uni/tn-
infra/ap-access","lcOwn":"local","modTs":"2016-09-07T08:17:20.503+00:00","monPolDn":"uni/tn-
common/monepg-
default","name":"access","ownerKey":"","ownerTag":"","prio":"unspecified","status":"","uid":
"0"},

"children":[{"healthInst":{"attributes":
{"childAction":"","chng":"0","cur":"100","maxSev":"cleared","prev":"100","rn":"health","stat
us":"","twScore":

"100","updTs":"2016-09-07T08:39:35.531+00:00"}}}]}
```

EPG Health Event

```
[Cisco_ACI_EPG_Health]: {"attributes":
{"childAction":"","configIssues":"","configSt":"applied","descr":"","dn":"uni/tn-infra/ap-
access/epg-
default","isAttrBasedEPg":"no","lcOwn":"local","matchT":"AtleastOne","modTs":"2016-09-
07T08:17:20.503+00:00","monPolDn":"uni/tn-common/monepg-
default","name":"default","pcEnfPref":"unenforced","pcTag":"16386","prio":"unspecified",

"scope":"16777199","status":"","triggerSt":"triggerable","txId":"5764607523034234882","uid":
"0"},"children":[{"healthInst":{"attributes":
{"childAction":"","chng":"0","cur":"100","maxSev":"cleared","prev":"100","rn":"health","stat
us":"",

"twScore":"100","updTs":"2016-09-07T08:39:35.549+00:00"}}}]
```

Fault Record Event

```
[Cisco_ACI_Fault_Record]: ,"created":"2016-09-
05T08:00:41.313+00:00","delegated":"no","delegatedFrom":"","descr":

"Controller3isunhealthybecause:DataLayerPartiallyDegradedLeadership","dn":"subj-
[topology/pod-1/node-1/av/node-3]/fr-
4294967583","domain":"infra","highestSeverity":"critical","id":"4294967583","ind":"modificat
ion",

"lc":"soaking","modTs":"never","occur":"1","origSeverity":"critical","prevSeverity":"critica
l",

"rule":"infra-wi-node-
health","severity":"critical","status":"","subject":"controller","type":"operational"}
```

Event Record Event

```
[Cisco_ACI_Event_Record]: {"attributes":{"affected":"topology/pod-1/node-2/lon/svc-ifc_
dhcpd","cause":"state-change","changeSet":"id:ifc_
dhcpd,leCnnct:undefined,leNonOptCnt:undefined,leNotCnnct:undefined,name:ifc_
dhcpd","childAction":"","code":"E4204979","created":"2016-09-
05T07:57:37.024+00:00","descr":"Allshardsofserviceifc_
dhcpdhaveconnectivitytotheleaderreplicaintheCluster.","dn":"subj-[topology/pod-1/node-
2/lon/svc-ifc_dhcpd]/rec-8589934722","id":"8589934722","ind":"state-
transition","modTs":"never","severity":"info","status":"","trig":"oper","txId":

"18374686479671623682","user":"internal"}
```

Log Record Event

```
[Cisco_ACI_Log_Record]: {"attributes":{"affected":"uni/userext/user-
admin","cause":"unknown","changeSet":"","childAction":"","clientTag":"","code":"generic","cr
eated"

:"2016-09-05T07:56:25.825+00:00","descr":"From-198.18.134.150-client-type-REST-

Success","dn":"subj-[uni/userext/user-admin]/sess-
4294967297","id":"4294967297","ind":"special","modTs":"never","severity":"info","status":"",
"systemId":"1","trig":

"login,session","txId":"0","user":"admin"}
```

Configuration Change Event

```
[Cisco_ACI_Configuration_Chang]: {"attributes":{"affected":"uni/tn-CliQr/out-CliQr-Prod-
L3Out/instP-CliQr-Prod-L3Out-
EPG/rscustQosPol","cause":"transition","changeSet":"","childAction":"","clientTag":"","code"
:"E4206266",

"created":"2016-09-05T07:56:27.099+00:00","descr":"RsCustQosPolcreated","dn":"subj-[uni/tn-
CliQr/out-CliQr-Prod-L3Out/instP-CliQr-Prod-L3Out-EPG/rscustQosPol]/mod-
4294967308","id":"4294967308","ind":"creation","modTs":"never","severity":"info","status":""
,"trig":"config","txId":

"7493989779944505526","user":"admin"}}
```

Fortinet FortiInsight

FortiInsight is a unique data security and threat detection solution that delivers advanced threat hunting to help you spot, respond to, and manage risky behaviors that put your business-critical data at risk. It combines powerful and flexible Machine Learning with detailed forensics around user actions to bring focus to the facts more rapidly than other solutions.

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration in FortiInsight
- Configuration in FortiSIEM
- Sample Events

What is Discovered and Monitored

Protocol	Information collected	Used for
FortiInsight API	Policy based alerts and AI based alerts	Data security, threat protection

This feature allows FortiSIEM to get Policy-based alerts and AI-based alerts from FortiInsight.

Event Types

In **RESOURCES > Event Types**, enter "FortiInsight" in the main content panel **Search...** field to see the event types associated with this device.

Rules

No defined rules.

Reports

In **RESOURCES > Reports**, enter "FortiInsight" in the main content panel **Search...** field to see the rules associated with this device.

Configuration in FortiInsight

Get an API Key in FortiInsight

Complete these steps in the FortiInsight UI:

1. Login to FortiInsight.
2. Select **Admin > Account** from the left menu.

3. Click **New API Key** to open the New API Key dialog box.
4. Enter a descriptive **Name**.
5. Click **Save** to generate the API key. This will download a file containing the API key information (**Client ID**, **Client Secret**, and **Name**). Make a note of these values; you will need them when you configure FortiSIEM.

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	Fortinet FortiSIEM
Access Protocol	FortiInsight API
Pull Interval	The interval in which FortiSIEM will pull events from FortiInsight. Default is 3 minutes.
Client ID	Access key for your FortiInsight instance.
Client Secret	Secret key for your FortiInsight instance
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your Fortinet FortiInsight credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiInsight.
5. To see the jobs associated with FortiInsight, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "FortiInsight" in the search box.

Sample Events

```
[FORTIINSIGHT_POLICY_ALERT] = {"description":"","events":[{"act":"file
downloaded","app":"chrome.exe","childId":null,"d":"2019-03-
18T13:22:24.344+00:00","id":null,"m":"uqP","mn":{"dh":"tcp://server-10-230-2-
153.lhr5.r.cloudfront.net","dip":"10.1.1.76","dp":61024,"ext":".mkv","fp":"c:\\users\\Admini
strator\\documents\\secret\\prototypedemo1.mkv","fs":2307792448,"loc":
```

```
{"altCode":null,"city":"Augsburg","code":"DE","country":"Germany","latitude":"48.3718","long
itude":"10.8925"},"p":"tcp-ip-
4","sip":"78.47.38.226","sp":443,"ts":1460},"r":"c:\\users\\Administrator\\documents\\secret
\\prototypedemo1.mkv-> tcp://server-54-230-2-153.lhr5.r.cloudfront.net:443","u":"acmeltd__
engineer2"}],"extendedEvents":[{"act":"file
downloaded","app":"chrome.exe","childId":null,"d":"2019-03-
18T13:22:24.344+00:00","id":null,"latestHostname":"mimas","latestIp":"10.10.0.1","m":"uqP","
mn":{"dh":"tcp://server-54-230-2-
153.lhr5.r.cloudfront.net","dip":"10.1.1.76","dp":61024,"ext":".mkv","fp":"c:\\users\\Admini
strator\\documents\\secret\\prototypedemo1.mkv","fs":2307792448,"loc":
{"altCode":null,"city":"Augsburg","code":"DE","country":"Germany","latitude":"48.3718","long
itude":"10.8925"},"p":"tcp-ip-
4","sip":"78.47.38.226","sp":443,"ts":1460},"r":"c:\\users\\Administrator\\documents\\secret
\\prototypedemo1.mkv-> tcp://server-10-230-2-
153.lhr5.r.cloudfront.net:443","resolvedUsername":"","u":"acmeltd__
engineer2"}],"id":"AWmQ98PYg7b_-i6_5Rvg","labels":[""],"policyId":"default_
6COnUMjTCB8N","policyName":"Browser Download","regimes":
["ZoneFox"],"serverIp":"52.209.49.52","serverName":"fortisiemtest.dev.fortiinsight.cloud","s
everity":10,"status":"New","time":"2019-03-18T13:22:29.473715+00:00"}
```

Fortinet FortiManager

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring

Event Types

Regular monitoring events

- PH_DEV_MON_SYS_CPU_UTIL
- PH_DEV_MON_SYS_MEM_UTIL
- PH_DEV_MON_SYS_DISK_UTIL
- PH_DEV_MON_NET_INTF_UTIL

Rules

Regular monitoring rules

Reports

Regular monitoring reports

Configuration

Configuring FortiManager to send Local Logs to Syslog Server

To configure FortiManager to sent local logs to the syslog server, take the following steps:

1. Go to *System Settings* > *Advanced* > *Syslog Server* to configure syslog server settings.
2. Double-click on a server, right-click on a server, and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Syslog Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

Configuring FortiManager for Security and Compliance and Perf Logs

To configure FortiManager for Security and Compliance and Perf Logs, take the following steps:

1. Go to *System Settings* > *Advanced* > *SNMP* to configure the SNMP agent.
2. Select an SNMP Agent to enable/Select the *Enable* checkbox.
3. Configure the SNMP Agent.

Configure an SNMPv3 User

1. Go to *System Settings* > *Advanced* > *SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v3* section, click *Create New* in the toolbar. The *New SNMP User* pane opens. Enter the following:
    a. In the *User Name* field, enter "fortisiem".
    b. In *Security Level*, select *Authentication, Privacy*.
    c. Select *Authentication Algorithm (SHA1, MD5)* the *Private Algorithm (AES, DES)*.
    d. Select *SHA1* and enter the password.
    e. Select *AES* and enter the password.
    f. Select *Queries* to enable, and leave the default port UDP to 161.
    g. In the *Notification Hosts* field, enter the FortiSIEM collector IP address.
    h. In *SNMP Event*, select all events.
    i. Click *Save*.

You can now configure FortiSIEM to communicate with FortiManager. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide. For **Device Type** Fortinet FortiManager, see Access Credentials.

HP Integrated Lights Out (iLO)

Event Types

In **ADMIN > Device Support > Event Types**, search for "hp-" and look for HP iLO in the Device Type column to see the event types associated with this device. In FortiSIEM 6.3.0, there are 25 new event types and 500+ generic HP SNMP trap event types.

Rules

No specific rules are available.

Reports

No specific reports are available.

Configuration

For the latest HP iLO documentation, see https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-a00026111en_us#N1050D.

SNMPv1 Traps Configuration

Configure SNMP Settings

To configure SNMP, take the following steps:

1. In the navigation tree, click **Management**.
2. In the SNMP Settings section, enter the following values:
   - System Location
   - System Contact
   - System Role
   - System Role Detail
   - Read Community 1
   - Read Community 2
   - Read Community 3

3. Click **Apply**.
   Note: More information is available here.

Add SNMP Alert Destinations

1. In the navigation tree, click **Management.**
2. In the **SNMP Alert Destinations** section, click **New**, and enter the following values.
   - SNMP Alert Destination
   - Trap Community
   - SNMP Protocol
   - SNMPv3 User
3. Click **Add.**
   Note: More information is available here.

Configure SNMP Alerts

1. In the navigation tree, click **Management.**
2. In the **SNMP Alerts** section, configure **Trap Source Identifier** by selecting **iLO Hostname** or **OS Hostname**.
3. Configure the following values:
   - iLO SNMP Alerts
   - SNMPv1
   - Cold Start Trap Broadcast
   - Periodic HSA Trap Configuration

   Click **Apply** to save.
   Note: More information is available here.

Remote Desktop

FortiSIEM supports this remote desktop application for discovery and monitoring.

- Citrix Receiver (ICA)

Citrix Receiver (ICA)

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
WMI		From `PH_DEV_MON_APP_ICA_SESS_MET`: • ICA Latency Last Recorded • ICA Latency Session Average • ICA Latency Session Deviation • ICA Input Session Bandwidth • ICA Input Session Line Speed • ICA Input Session Compression • ICA Input Drive Bandwidth • ICA Input Text Echo Bandwidth • ICA Input SpeedScreen Data Bandwidth • Input Audio Bandwidth • ICA Input VideoFrame Bandwidth • ICA Output Session Bandwidth • ICA Output Session Line Speed • ICA Output Session Compression • ICA Output Drive Bandwidth • ICA Output Text Echo Bandwidth • ICA Output SpeedScreen Data Bandwidth • ICA Output Audio Bandwidth • ICA Output VideoFrame Bandwidth	

Event Types

In **ADMIN > Device Support > Event Types**, search for "citrix ICA" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "citrix ICA" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- WMI

WMI

Required WMI Class

Make sure the WMI class `Win32_PerfRawData_CitrixICA_ICASession` is available on the host machine for Citrix ICA.

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- Creating a Generic User Who Does Not Belong to the Local Administrator Group
- Creating a User Who Belongs to the Domain Administrator Group

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add**.
6. Find the user you created, and then click **OK.**
   This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed.**
5. Click **OK.**
6. Under **Access Permissions,** click **EditDefault**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed.**
8. Click **OK.**
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.

12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Enable remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Pane > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user for the @accelops.com domain.
   For example, **YJTEST@accelops.com**.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties.**
3. Select the **Security** tab.

4. Expand the **Root** directory and select **CIMV2.**
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced.**
8. Select the user you created for the monitoring account, and then click **Edit.**
9. In the **Apply onto** menu, select **This namespace and subnamespaces.**
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services.**
13. Select **Windows Management Instrumentation**, and then click **Restart.**

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run.**
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception.**
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall.**
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and the click **OK.**

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Source Code Control

FortiSIEM supports the GitHub and GitLab Source Code Control tools for log collection via an API.

- GitHub
- GitLab API
- GitLab CLI

GitHub

Integration Points

Protocol	Information collected	Used for
GitHub API	Logs from the GitHub Service	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "GitHub" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "GitHub" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "GitHub" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Configuring GitHub Server

Create an account to be used for FortiSIEM communication.

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access.

1. Login to FortiSIEM.
2. Go to **ADMIN > Setup** > **Credentials**.

3. In **Step 1: Enter Credentials**, click **New** to create a GitHub credential.
4. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	GitHub.com GitHub
Access Protocol	GitHub API
Pull Interval	The interval in which FortiSIEM will pull events. Default is 5 minutes.
Password Config	See Password Configuration
User Name and Password	Enter the user name and password for the account created while Configuring GitHub Server.
Organization	Choose the Organization if it is an MSP deployment and the same credential has to be used for multiple customers.
Description	Description of the device

5. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Set **IP/Host Name** to the IP address of the GitHub Server.
   b. Select the **Credential** created in steps 3 and 4.
   c. Click **Save**.
6. Select the entry in step 3 above and click the **Test** drop-down list, and select **Test Connectivity**.
7. After **Test Connectivity** succeeds, an entry will be created in **ADMIN > Setup** > **Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from GitHub server using the API.

To test for received GitHub events:

1. Go to **ADMIN > Setup** > **Pull Events**.
2. Select the GitHub entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from GitHub in the last 15 minutes. You can modify the time interval to get more events.

GitLab API

- Integration Points
- Event Types
- Rules
- Reports
- Syslog Integration
- API Integration
- Configuring GitLab Server
- Configuring FortiSIEM for GitLab API
- Sample Event

Integration Points

Protocol	Information collected	Used For
syslog	15 Log files including production.log and application.log – over 130 event types pre-fixed with 'GitLab-'	Security and Compliance
API	Code commit, Changes to Projects, Branches, Tag, DiscussionNoted, Tag, Issues, Snippets, Repositories, User created, deleted, modified.	Security and Compliance

Event Types

In **RESOURCES > Event Types**, enter "GitLab" in the main content panel **Search...** field to see the events associated with this device.

Rules

No defined rules.

Reports

In **RESOURCES > Reports**, enter "GitLab" in the main content panel **Search...** field to see the reports associated with this device.

Syslog Integration

Configure GitLab to send syslog to FortiSIEM via UDP on port 514. See here for details.

FortiSIEM will automatically detect GitHLab log patterns and parse the logs. Currently, the following log files are parsed: api_json.log, application.log, gitaly, gitlab-monitor, gitlab-shell.log, gitlab-workhorse.log, gitlab_ access.log,production.log, production_json.log, Prometheus, Redis, remote-syslog, sidekiq, sidekiq_exporter.log, unicorn_stderr.log.

Currently, over 134 GitLab event types are parsed. To see the event types:

1. Login to FortiSIEM.
2. Go to **RESOURCES** > **Event Types**.
3. Search for "GitLab".

Use cases covered via syslog:

- Failed and Successful Login
- Git command execution
- Git API requests

To test for received GitLab events received via syslog:

1. Login to FortiSIEM.
2. Go to **ANALYTICS**.
3. Click the **Edit Filters and Time Range...** field:
   a. Choose the **Event Attribute** option.
   b. Create the Search condition
      Attribute: Event Type
      Operator: CONTAIN
      Value: GitLab
   c. Change **Time Range** to be Last 1 Hour
   d. Click **Apply & Run**.
4. See the GitLab events on the GUI.

API Integration

FortiSIEM can also pull logs from GitLab using GitLab API.

Currently, over 134 GitLab event types are parsed. To see the event types:

1. Login to FortiSIEM.
2. Go to **RESOURCES** > **Event Types**.
3. Search for "GitLab".

Use cases covered via API:

- Code commit – note that the current API does not capture committed files.
- Changes to Projects, Branches, Tag, DiscussionNoted, Tag, Issues, Snippets, Repositories etc
- User created, deleted, modified

For more details, see here.

Configuring GitLab Server

Create a personal access token to be used for FortiSIEM communication.

1. Login to your GitLab account.
2. Go to your **Profile settings**.

3. Go to **Access tokens**.
4. Choose a name and optionally an expiry date for the token.
5. Choose the desired scopes: **api** is required.
6. Click **Create Personal Access Token**. Save the personal access token in your local system. Note that once you leave or refresh the page, you won't be able to access it again.

For more details, see here.

Configuring FortiSIEM for GitLab API

Use the Personal Access Token in Configuring GitLab Server to enable FortiSIEM access.

1. Login to FortiSIEM.
2. Go to **ADMIN > Setup** > **Credentials**.
3. In **Step 1: Enter Credentials**, click **New** to create a GitLab credential.
4. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	GitLab GitLab (Vendor = GitLab, Model = Gitlab)
Access Protocol	GitLab API
Pull Interval	The interval in which FortiSIEM will pull events from GitLab. Default is 5 minutes.
Password Config	Manual
Account Name	Enter an account name.
Personal Access Token	Enter the token you obtained in Configuring GitLab Server.
Description	Description of the device

5. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. In **IP/Host Name**, enter the **IP** of GitLab Server.
   b. Select the **Credential** created in step 4 above.
   c. Click **Save**.
6. Select the entry in step 3 above, click the **Test** drop-down list and select **Test Connectivity**. Once successful, an entry will be created in **ADMIN > Setup** > **Pull Events**. FortiSIEM will start to pull events from GitLab using the API.

To test for received GitLab events:

1. Go to **ADMIN > Setup** > **Pull Events**.
2. Select the GitLab entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from GitLab in the last 15 minutes. You can modify the time interval to get more events.

Sample Event

```
[GITLAB_EVENT_DATA] = {"action_name":"pushed to","author":{"avatar_
url":"https://abc.cda.com/avatar/62e30f8b2d3cbc60ed22c217c5fa4e57?s=80&d=identicon","id
":185,"name":"user1","state":"active","username":" user1","web_
url":"https://dac.com/gitmirror"},"author_id":185,"author_username":" user1","created_
at":"2018-11-13T22:30:30.340Z","project_id":553,"push_data":{"action":"pushed","commit_
count":2,"commit_from":"da5a4fd97fd1f6b7c5a8611c12592eb5e9ff9e2b","commit_title":"Merge
\"Fix bizservice popup display issue and switching org in bizs...","commit_
to":"30d863ece3957aacc95ec45c7663c426c73f38f2","ref":"releases/FCS5_2_1","ref_
type":"branch"},"serverIp":"172.30.35.11","serverName":"abc.com","target_
id":null,"target_iid":null,"target_title":null,"target_type":null}
```

GitLab CLI

Events that are obtained with the GitLab REST API do not contain up-to-date information. To avoid this limitation, FortiSIEM uses the GitLab CLI to obtain events from the GitLab server in real time.

- Integration Points
- Event Types
- Rules
- Reports
- Generate an SSH Key in FortiSIEM
- Configure an SSH Key in GitLab
- Configuration in FortiSIEM
- Sample Events

Integration Points

Protocol	Information collected	Used for
GIT CLI	Git commit history	Security and Compliance

Event Types

In **RESOURCES > Event Types**, enter "GitLab" in the main content panel **Search...** field to see the events associated with this device.

Rules

No defined rules.

Reports

In **RESOURCES > Reports**, enter "GitLab" in the main content panel **Search...** field to see the reports associated with this device.

Generate an SSH Key in FortiSIEM

Generate an SSH key for FortiSIEM. The key will allow you to access the GitLab by using Git commands. Use the following command to generate the public key file and the private key file in the `/opt/phoenix/bin/.ssh/` directory.

```
ssh-keygen -t rsa -b 4096 -C "root@localhost"
```

Configure an SSH Key in GitLab

Complete these steps to install the SSH key in the GitLab server:

1. Login to your GitLab account.
2. Select **Settings** from your account drop-down list.
3. Select the **SSH Keys** tab.
4. Add the public part of the key, for example:
   `/opt/phoenix/bin/.ssh/id_rsa.pub`
5. Click **Add Key**.
6. Install Git, for example:
   `yum install git`

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	GitLab GitLab
Access Protocol	GIT CLI
Pull Interval	The interval in which FortiSIEM will pull events from GitLab. Default is 5 minutes.
Local Path to Clone	The path to the location on your system where the repository will be downloaded. In the case of very large repositories, this gives users the opportunity to specify a location on an external device.
Repositories	The address of the repository in Git. You can enter multiple repositories, separated by whitespaces.
Description	Description of the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter an IP or an IP range in the **IP/Host Name** field.
   b. Select the name of your GitLab credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. With your Credentials entry selected from Step 3, click the **Test** drop-down list and select **Test Connectivity** to test the connection to GitLab CLI.
5. To see the jobs associated with GitLab, select **ADMIN > Setup > Pull Events**.
6. To see the received events, select **ANALYTICS**, then enter "GitLab" in the search box.

Sample Events

```
[PH_DEV_MON_GIT_COMMIT]: [deviceTime]=1547013028,[user]="abc",
[exchMboxName]="abc@fortinet.com",
[hashCode]="fa408380aa4296d13aeb24418164994eea2c2737",
[preHashCode]="d9cd6e31346611a4f75dc7fe768f6202a46dd7e6",[title]="Add new file",
[details]="",[updateCount]="1",[deleteCount]="0",[filePath]="testfile2",
[fileType]="testfile2",[repoURL]="git@dops-git.fortinet-us.com:abc/testproject_mei_
willremove.git"
```

Unified Communication Server Configuration

FortiSIEM supports these VoIP servers for discovery and monitoring.

- Avaya Call Manager
- Cisco Call Manager
- Cisco Contact Center
- Cisco Presence Server
- Cisco Tandeberg Telepresence Video Communication Server (VCS)
- Cisco Telepresence Multipoint Control Unit (MCU)
- Cisco Telepresence Video Communication Server
- Cisco Unity Connection

Avaya Call Manager

- What is Discovered and Monitored
- Event Types
- Configuration
- Configure FortiSIEM to Receive CDR Records from Avaya Call Manager
- Configure Avaya Call Manager to Send CDR Records to FortiSIEM
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**System metrics:** Uptime, Interface utilization	Performance Monitoring
SFTP		**Call Description Records (CDR):** Calling Phone IP, Called Phone IP, Call Duration	Performance and Availability Monitoring

Event Types

Avaya-CM-CDR: Avaya CDR Records

Configuration

- SNMP
- SFTP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

SFTP

SFTP is used to send Call Description Records (CDRs) to FortiSIEM.

Configure FortiSIEM to Receive CDR Records from Avaya Call Manager

1. Log in to your FortiSIEM virtual appliance as `root` over SSH.
2. Change the directory.
   ```
   cd /opt/phoenix/bin
   ```

3. Create an FTP account for user **ftpuser** with the home directory `/opt/phoenix/cache/avayaCM/<call-manager-ip>`. If this is the first time you have created a Call Manager definition, you will be prompted for the ftpuser password. When you create subsequent Call Manager definitions, the same password will be used, and you will see a Success message when the definition is created.
4. The CDR records do not have field definitions, but only values. Field definitions are needed to properly interpret the values. Make sure that the CDR fields definitions matches the default one supplied by FortiSIEM in `/opt/phoenix/config/AvayaCDRConfig.csv`.
   FortiSIEM will interpret the CDR record fields according to the field definitions specified in:`/opt/phoenix/config/AvayaCDRConfig.csv` and generate events like the following:

   ```
   Wed Feb 4 14:37:41 2015 1.2.3.4 FortiSIEM-FileLog-AvayaCM [Time of day-hours]="11" [Time of day-minutes]="36" [Duration-hours]="0" [Duration-minutes]="00" [Duration-tenths of minutes]="5" [Condition code]="9" [Dialed number]="5908" [Calling number]="2565522011" [FRL]="5" [Incoming circuit ID]="001" [Feature flag]="0" [Attendant console]="8" [Incoming TAC]="01 1" [INS]="0" [IXC]="00" [Packet count]="12" [TSC flag]="1"
   ```

Configure Avaya Call Manager to Send CDR Records to FortiSIEM

1. Log in to Avaya Call Manager.
2. Send CDR records to FortiSIEM by using this information

Field	Value
Host Name/IP Address	*<FortiSIEM IP Address>*
User Name	ftpuser
Password	*<The password you created for ftpuser>*
Protocol	SFTP
Directory Path	`/opt/phoenix/cache/avayaCM/<call-manager-ip>`

Settings for Access Credentials in FortiSIEM

See Access Credentials to set access and protocol for SMTP, SSH, and Telnet.

Cisco Call Manager

- What is Discovered and Monitored
- Event Types
- Rules
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**System metrics:** Uptime, CPU utilization, Memory utilization, Disk utilization, Interface utilization, Process count, Per process: CPU utilization, Memory utilization	Performance Monitoring
SNMP	VoIP phones and registration status	**Call Manager metrics:Global Info**: VoIP phone count, Gateway count, Media Device count, Voice mail server count and SIP Trunks count broken down by Registered/Unregistered/Rejected status (FortiSIEM Event Type: PH_DEV_MON_CCM_GLOBAL_INFO) **SIP Trunk Info**: Trunk end point, description, status (FortiSIEM Event Type: PH_DEV_MON_CCM_SIP_TRUNK_STAT) **SIP Trunk Addition, Deletion:** FortiSIEM Event Type: PH_DEV_MON_CCM_NEW_SIP_TRUNK, PH_DEV_MON_CCM_DEL_SIP_TRUNK **Gateway Status Info:** Gateway name, Gateway IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_GW_STAT) **Gateway Status Change, Addition, Deletion:** FortiSIEM Event Type: PH_DEV_MON_CCM_GW_STAT_CHANGE, PH_DEV_MON_CCM_NEW_GW, PH_DEV_MON_CCM_DEL_GW**H323 Device Info:** H323 Device name, H323 Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_H323_STAT) **Gateway Status Change, Addition, Deletion**: FortiSIEM Event Type: PH_DEV_MON_CCM_H323_STAT_CHANGE, PH_DEV_MON_CCM_NEW_H323, PH_DEV_MON_CCM_DEL_H323 **Voice Mail Device Info:** Voice Mail Device name, Voice Mail Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_VM_STAT)	Availability Monitoring

Protocol	Information discovered	Metrics collected	Used for
		Voice Mail Device Status Change, Addition, Deletion: FortiSIEM Event Type: PH_DEV_MON_CCM_VM_STAT_CHANGE, PH_DEV_MON_CCM_NEW_VM, PH_DEV_MON_CCM_DEL_VM **Media Device Info:** Media Device name, Media Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_MEDIA_STAT) **Media Device Status Change, Addition, Deletion:** FortiSIEM Event Type: PH_DEV_MON_CCM_MEDIA_STAT_CHANGE, PH_DEV_MON_CCM_NEW_MEDIA, PH_DEV_MON_CCM_DEL_MEDIA **Computer Telephony Integration (CTI) Device Info:** CTI Device name, CTI Device IP, description, status (FortiSIEM Event Types: PH_DEV_MON_CCM_CTI_STAT) **CTI Device Status Change, Addition, Deletion:** FortiSIEM Event Type: PH_DEV_MON_CCM_CTI_STAT_CHANGE, PH_DEV_MON_CCM_NEW_CTI, PH_DEV_MON_CCM_DEL_CTI	
WMI (for Windows based Call Managers)	Application type, service mappings	**Process level metrics:** Per process: Uptime, CPU utilization, Memory utilization, Read I/O KBytes/sec, Write I/O KBytes/sec	Performance Monitoring
SFTP		**Call Description Records (CDR):** Calling Phone IP, Called Phone IP, Calling Party Number, Original Called Party Number, Final Called Party Number, Call Connect Time, Call Disconnect Time, Call Duration **Call Management Records (CMR)**: Latency, Jitter, Mos Score - current, average, min, max for each call in CDR	Performance and Availability Monitoring
Syslog		Syslog messages from Cisco Call Manager as well as Cisco Unified Real Time Monitoring Tool (RTMT)	

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco_uc" and "cisco_uc_rtmt" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "cisco call manager" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

- SNMP
- WMI (for Call Manager installed under Windows)
- SFTP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

WMI (for Call Manager installed under Windows)

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- Creating a Generic User Who Does Not Belong to the Local Administrator Group
- Creating a User Who Belongs to the Domain Administrator Group

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add.**
6. Find the user you created, and then click **OK.**
   This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed.**
5. Click **OK**.
6. Under **Access Permissions,** click **EditDefault**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed.**

8. Click **OK.**
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Enable remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Pane > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user for the @accelops.com domain.
   For example, **YJTEST@accelops.com**.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2.**
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced.**
8. Select the user you created for the monitoring account, and then click **Edit.**
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart.**

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run.**
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall.**
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception.**
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall.**
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall.**
3. Select **Windows Management Instrumentation**, and the click **OK.**

SFTP

SFTP is used to send Call Description Records (CDRs) to FortiSIEM.

- Configure FortiSIEM to Receive CDR Records from Cisco Call Manager
- Configure Cisco Call Manager to Send CDR Records to FortiSIEM

Configure FortiSIEM to Receive CDR Records from Cisco Call Manager

1. Log in to your FortiSIEM virtual appliance as `root` over SSH.
2. Change the directory.

   ```
   cd /opt/phoenix/bin
   ```

3. Run `./phCreateCdrDestDir <call-manager-ip>`.
   This creates an FTP account for user **ftpuser** with the home directory `/opt/phoenix/cache/ccm/<call-manager-ip>`. If this is the first time you have created a Call Manager definition, you will be prompted for the ftpuser password. When you create subsequent Call Manager definitions, the same password will be used, and you will see a Success message when the definition is created.
4. Switch user to admin by issuing "su - admin"
5. Modify phoenix_config.txt entry

   ```
   ccm_ftp_directory = /opt/phoenix/cache/ccm
   ```

6. Restart phParser by issuing "killall -9 phParser"

Configure Cisco Call Manager to Send CDR Records to FortiSIEM

1. Log in to Cisco Call Manager.
2. Go to **Tools > CDR Management Configuration**.
   The CDR Management Configuration window will open.
3. Click **Add New**.
4. Enter this information.
5.

Field	Value
Host Name/IP Address	<FortiSIEM IP Address>
User Name	ftpuser
Password	<The password you created for ftpuser>
Protocol	SFTP
Directory Path	/opt/phoenix/cache/ccm/<call-manager-ip>

6. Click **Save**.

Settings for Access Credentials

See Access Credentials to set access and protocol for SMTP, SSH, and Telnet.

Cisco Contact Center

- What is Discovered and Monitored
- Event Types
- Rules
- Configuration
- Setting Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**System metrics:** CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization, Install software change	Performance Monitoring
SSH		Disk I/O monitoring	

Event Types

There are no event types defined specifically for this device.

Rules

In **RESOURCES > Rules**, search for "cisco contact center" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

- SNMP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Setting Access Credentials

See Access Credentials to set access and protocol for SMTP, SSH, and Telnet.

Cisco Presence Server

- What is Discovered and Monitored
- Event Types
- Configuration
- Setting Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**System metrics:** CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization, Install software change	Performance Monitoring
SSH		Disk I/O monitoring	

Event Types

There are no event types defined specifically for this device.

Configuration

- SNMP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Setting Access Credentials

See Access Credentials to set access and protocol for SMTP, SSH, and Telnet.

Cisco Tandeberg Telepresence Video Communication Server (VCS)

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**System metrics:** CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization, Install software change	Performance Monitoring
SSH		Disk I/O monitoring	

Event Types

There are no event types defined specifically for this device.

Configuration

- SNMP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Cisco Telepresence Multipoint Control Unit (MCU)

- What is Discovered and Monitored
- Event Types
- Configuration
- Setting Access Credentials

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Cisco Tandeberg VCS

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**System metrics:** Uptime, Interface utilization	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco telepresence" to see the event types associated with this device.

Configuration

- SNMP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide

Setting Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic

Setting	Value
Access Protocol	SNMP
Community String	<your own>

Cisco Telepresence Video Communication Server

- What is Discovered and Monitored
- Event Types

What is Discovered and Monitored

Protocol	Logs parsed	Used for
Syslog	Call attempts, Call rejects, Media stats, Request, response, Search	Log Analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "Cisco-TVCS" to see the event types associated with this device.

Cisco Unity Connection

- What is Discovered and Monitored
- Event Types
- Rules
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**System metrics:** CPU utilization, Memory utilization, Disk utilization, Interface utilization, Hardware Status, Process count, Process level CPU and memory utilization	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco unity" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "cisco unity" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

- SNMP

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

See Access Credentials to set access and protocol for SMTP, SSH, and Telnet.

Web Server

FortiSIEM supports these web servers for discovery and monitoring.

- Apache Web Server
- Microsoft IIS for Windows 2000 and 2003
- Microsoft IIS for Windows 2008
- NGINX Web Server

Apache Web Server

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Define the Apache Log Format
- Apache Syslog Log Format
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**Process level metrics:** CPU utilization, Memory utilization	Performance Monitoring
HTTP(S) via the mod-status module		**Apachemetrics**: Uptime, CPU load, Total Accesses, Total Bytes Connections, Requests/sec, Bytes/sec, Bytes/req, Busy Workers, Idle Workers	Performance Monitoring
Syslog	Application type	**W3C access logs**: attributes include Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "apache" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "apache" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

The Apache Web Server Configuration instructions utilizes a reference point for where Apache installs by default. Based on your own configuration, Apache may be installed in the following locations:

```
/etc
```

```
/etc/httpd
```

```
/usr/local
```

Adjust your configuration according to your installed Apache directory.

- SNMP
- HTTPS
- Syslog

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

HTTPS

To communicate with FortiSIEM over HTTPS, you must configure the mod_status module in your Apache web server.

1. Log in to your web server as an administrator.
2. Open the configuration file `/etc/Httpd.conf`.
3. Modify the file as shown in these code blocks, depending on whether you are connecting over HTTP without authentication, or over HTTPS with authentication.
   Without Authentication

   ```
   LoadModule status_module modules/mod_status.so
   ...
   ExtendedStatus on
   ...
   #Configuration without authentication
   <Location /server-status>       SetHandler server-status
       Order Deny,Allow
       Deny from all
       Allow from .foo.com
   </Location>
   ```

   With Authentication

   ```
   LoadModule status_module modules/mod_status.so
   ...
   ExtendedStatus on
   ...
   #Configuration with authentication
   <Location /server-status>      SetHandler server-status
      Order deny,allow
      Deny from all
      Allow from all
      AuthType Basic
      AuthUserFile /etc/httpd/account/users
      AuthGroupFile /etc/httpd/account/groups
      AuthName "Admin"      Require group admin
      Satisfy all
   </Location>
   ```

4. If you are using authentication, you will have to add user authentication credentials.
   a. Go to `/etc/httpd`, and if necessary, create an `account` directory.
   b. In the `account` directory, create two files, `users` and `groups`.
   c. In the `groups` file, enter `admin:admin`.

   d. Create a password for the admin user.

      ```
      htpasswd --c users admin
      ```

5. Reload Apache.

   ```
   /etc/init.d/httpd reload
   ```

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

Install and configure Epilog application to send syslog to FortiSIEM

1. Download Epilog from snare, information to download here, and install it on your Windows Server.
2. For Windows, launch Epilog from Start→All Programs→InterSect Alliance→Epilog for windows
3. For Linux, enter `http://<yourApacheServerIp>:6162`
4. Configure Epilog application as follows
   a. Go to Log Configuration. Click the Add button and add the following log files to be sent to FortiSIEM
      - `/etc/httpd/logs/access_log`
      - `/etc/httpd/logs/ssl_access_log`

   b. Go to Network Configuration
      i. Set AO System IP(all-in-1 or collector) in Destination Server address (10.1.2.20 here);
      ii. Set 514 in Destination Port text area
      iii. Click Change Configuration to save the configuration

   c. Apply the Latest Audit Configuration. Apache logs will now sent to FortiSIEM in real time.

Define the Apache Log Format

You must define the format of the logs that Apache will send to FortiSIEM.

1. Open the file `/etc/httpd/conf.d/ssl.conf` for editing.
2. Add this line to the file.

   ```
   CustomLog logs/ssl_request_log combined
   ```

3. Uncomment this line in the file.

   ```
   #CustomLog logs/access_log common
   ```

4. Add this line to the file.

   ```
   CustomLog logs/access_log combined
   ```

5. Reload Apache.

   ```
   /etc/init.d/httpd reload
   ```

Apache Syslog Log Format

```
<142>Sep 17 13:27:37 SJ-Dev-S-RH-VMW-01.prospecthills.net ApacheLog   192.168.20.35 - -
[17/Sep/2009:13:27:37 -0700] "GET /icons/apache_pb2.gif HTTP/1.1" 200 2414
"http://192.168.0.30/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
```

```
2.0.50727)"<134>Mar  4 17:08:04 137.146.28.68 httpd: [ID 702911 local0.info] 192.168.20.38 -
- [04/Mar/2010:16:35:21 -0800] "GET /bugzilla-3.0.4/ HTTP/1.1" 200 10791 "-" "Mozilla/5.0
(Windows; U; Windows NT 6.0; en-US; rv:1.9.1.8) Gecko/20100202 Firefox/3.5.8 GTB6"<142>Sep
17 13:27:37 135.134.33.23 HTTP: [ID 702911 local0.info] 192.168.20.38 - -
[04/Mar/2010:16:35:21 -0800] "GET /bugzilla-3.0.4/ HTTP/1.1" 200 10791 "-" "Mozilla/5.0
(Windows; U; Windows NT 6.0; en-US; rv:1.9.1.8) Gecko/20100202 Firefox/3.5.8 GTB6"
```

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Settings for Apache Web Server HTTPS Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Settings for Apache Web Server HTTPS Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your Apache web server over https.

Setting	Value
Name	Apache-https
Device Type	generic
Access Protocol	HTTP or HTTPS
Port	80 (HTTP) or 443 (HTTPS)
URL	server-status?auto
User Name	The admin account you created when configuring HTTPS
Password	The password associated with the admin account

Microsoft IIS for Windows 2000 and 2003

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**Process level metrics:** CPU utilization, memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O **IIS metrics**: Current Connections, Max Connections, Sent Files, Received Files, Sent Bytes, Received Bytes, ISAPI Requests, Not Found Errors	Performance Monitoring
Windows Agent	Application type	**W3C access logs**: attributes include IIS Service Instance, Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft iis" to see the event types associated with this device.

Configuration

- SNMP
- WMI
- FortiSIEM Windows Agent

SNMP

See SNMP Configurations in the *Microsoft Windows Server Configuration* section.

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring IIS for FortiSIEM Windows Agent, see Configuring Windows IIS in the *Windows Agent Installation Guide*.

Settings for Access Credentials

See Setting Access Credentials in the *Microsoft Windows Server Configuration* section.

Microsoft IIS for Windows 2008

- What is Discovered and Monitored
- Event Types
- Configuration
- Setting Access Credentials
- Sample IIS Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**Process level metrics:** CPU utilization, memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics:** uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O **IIS metrics**: Current Connections, Max Connections, Sent Files, Received Files, Sent Bytes, Received Bytes, ISAPI Requests, Not Found Errors	Performance Monitoring
Windows Agent	Application type	**W3C access logs**: attributes include IIS Service Instance, Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft iis" to see the event types associated with this device.

Configuration

- SNMP
- WMI
- FortiSIEM Windows Agent

SNMP

See SNMP Configurations in the *Microsoft Windows Server Configuration* section.

WMI

See WMI Configurations in the *Microsoft Windows Server Configuration* section.

FortiSIEM Windows Agent

For information on configuring IIS for FortiSIEM Windows Agent, see Configuring Windows IIS in the *Windows Agent Installation Guide*.

Setting Access Credentials

See Setting Access Credentials in the *Microsoft Windows Server Configuration* section.

Sample IIS Syslog

```
<13>Oct  9 12:19:05 ADS-Pri.ACME.net IISWebLog              0              2008-10-09
19:18:43 W3SVC1 ADS-PRI 192.168.0.10 GET /iisstart.htm - 80 - 192.168.20.80 HTTP/1.1
Mozilla/5.0+(Windows;+U;+Windows+NT+5.1;+en-US;+rv:1.9.0.3)+Gecko/2008092417+Firefox/3.0.3 -
- 192.168.0.10 200 0 0 2158 368 156
<46>Mar 29 12:21:03 192.168.0.40 FTPSvcLog     0       2010-03-29 19:20:32 127.0.0.1 - MSFTPSVC1 FILER
127.0.0.1 21 [1]PASS IEUser@ - 530 1326 0 0 0 FTP - - - -
```

NGINX Web Server

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

The following protocols are used to discover and monitor various aspects of the NGINX webserver.

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**Process level metrics:** CPU utilization, Memory utilization	Performance Monitoring
Syslog		**W3C access logs**: attributes include Client IP, URL, User Agent, Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "nginx" to see the event types associated with this device.

Configuration

- SNMP
- Syslog
- Example NGINX Syslog

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example NGINX Syslog

```
<29>Jun 15 07:59:03 ny-n1-p2 nginx: "200.158.115.204","-","Mozilla/5.0 (Windows NT 5.1
WOW64; rv:9.0.1) Gecko/20100178 Firefox/9.0.1","/images/design/header-2-
logo.jpg","GET","http://wm-center.com/images/design/header-2-logo.jpg","200","0","/ypf-
cookie_auth/index.html","0.000","877","-","10.4.200.203","80","wm-center.com","no-cache, no-
store, must-revalidate","-","1.64","_","-","-"
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Blade Servers

FortiSIEM supports these blade servers for discovery and monitoring.

- Cisco UCS Server
- HP BladeSystem

Cisco UCS Server

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Settings for Access Credentials
- Sample Cisco UCS Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Cisco UCS API	Host name, Access IP, Hardware components - processors, chassis, blades, board, cpu, memory, storage, power supply unit, fan unit	**Chassis status**: Input Power, Input Avg Power, Input Max Power, Input Min Power, Output Power, Output Avg Power, Output Max Power, Output Min Power **Memory status**: Temp (C), Avg Temp (C), Max Temp (C), Min Temp (C) **Processor status**: Input Current, Input Avg Current, Input Max Current, Input Min Current, Temp (C), Avg Temp (C), Max Temp (C), Min Temp (C) **Power supply status**: Temp (C), Max Temp (C), Avg Temp (C), Min Temp (C), Input 210Volt, Avg Input 210Volt, Max Input 210Volt, Min Input 210Volt, Output 12Volt, Avg Output 12Volt, Max Output 12Volt, Min Output 12Volt, Output 3V3Volt, Avg Output 3V3Volt, Max Output 3V3Volt, Min Output 3V3Volt, Output Current, Avg Output Current, Max Output Current, Min Output Current, Output Power, Avg Output Power, Max Output Power,Min Output Power **Fan status**: Fan Speed, Average Fan Speed, Max Fan Speed, Min Fan Speed	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco ucs" to see the event types associated with this device.

Reports

In **RESOURCES > Reports**, search for "cisco ucs" to see the reports associated with this application or device.

Configuration

UCS XML API

FortiSIEM uses Cisco the Cisco UCS XML API to discover Cisco UCS and to collect hardware statistics. See the Cisco UCS documentation for information on how to configure your device to connect to FortiSIEM over the API.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	ucs
Device Type	Cisco UCS
Access Protocol	UCS API
Pull Interval (minutes)	5
Port	5988
User Name	The user name you set up in your UCS server to communicate with FortiSIEM
Password	The password associated with user name

Sample Cisco UCS Events

- Power Supply Status Event
- Processor Status Event
- Chassis Status Event
- Memory Status Event
- Fan Status Event

Power Supply Status Event

```
[PH_DEV_MON_UCS_HW_PSU_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,
[hostIpAddr]=10.1.2.36,[hwComponentName]=sys/chassis-1/psu-2,
[envTempdDegC]=47.764706,[envTempAvgDegC]=36.176472,[envTempMaxDegC]=47.764706,
[envTempMinDegC]=25.529411,[input210Volt]=214.294113,
[input210AvgVolt]=210.784317,[input210MaxVolt]=214.294113,[input210MinVolt]=207.823532,
[ouput12Volt]=12.188235,[ouput12AvgVolt]=12.109803,
[ouput12MaxVolt]=12.376471,[ouput12MinVolt]=11.905882,[ouput3V3Volt]=3.141176,
[ouput3V3AvgVolt]=3.374510,[ouput3V3MaxVolt]=3.458823,
[ouput3V3MinVolt]=3.141176,[outputCurrentAmp]=15.686275,[outputCurrentAvgAmp]=20.261436,
[outputCurrentMaxAmp]=24.509804,
[outputCurrentMinAmp]=15.686275,[outputPowerWatt]=191.188004,
[outputPowerAvgWatt]=245.736252,[outputPowerMaxWatt]=303.344879,
[outputPowerMinWatt]=191.188004
```

Processor Status Event

```
[PH_DEV_MON_UCS_HW_PROCESSOR_STAT]:[eventSeverity]=PHL_INFO, [hostName]=machine,
[hostIpAddr]=10.1.2.36,
[hwComponentName]=sys/chassis-1/blade-3/board/cpu-2,
[inputCurrentAmp]=101.101959,[inputCurrentAvgAmp]=63.420914,
[inputCurrentMaxAmp]=101.101959,[inputCurrentMinAmp]=44.580391,
[envTempdDegC]=5.788235,[envTempAvgDegC]=6.216993,[envTempMaxDegC]=6.431373,
[envTempMinDegC]=5.788235,
```

Chassis Status Event

```
[PH_DEV_MON_UCS_HW_CHASSIS_STAT]:[eventSeverity\]=PHL_INFO,[hostName]=machine,
[hostIpAddr]=10.1.2.36,[hwComponentName]=sys/chassis-1,
[inputPowerWatt]=7.843137,[inputPowerAvgWatt]=7.843137,[inputPowerMaxWatt]=7.843137,
[inputPowerMinWatt]=7.843137,
outputPowerWatt]=0.000000,[outputPowerAvgWatt]=0.000000,[outputPowerMaxWatt]=0.000000,
[outputPowerMinWatt]=0.000000
```

Memory Status Event

```
[PH_DEV_MON_UCS_HW_MEMORY_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,
[hostIpAddr]=10.1.2.36,
[hwComponentName]=sys/chassis-1/blade-1/board/memarray-1/mem-9,[envTempdDegC]=51.000000,
[envTempAvgDegC]=50.128208,
[envTempMaxDegC]=51.000000,[envTempMinDegC]=48.000000
```

Fan Status Event

```
[PH_DEV_MON_UCS_HW_FAN_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,
[hostIpAddr]=10.1.2.36,
[hwComponentName]=sys/chassis-1/fan-module-1-5/fan-2,[fanSpeed]=7800.000000,
[fanSpeedAvg]=7049.000000,
[fanSpeedMax]=8550.000000,[fanSpeedMin]=2550.00000
```

HP BladeSystem

- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Access IP, Hardware components - processors, chassis, blades, board, cpu, memory, storage, power supply unit, fan unit	**Hardware status**:Fan status, Power supply status, power enclosure status, Overall status	Availability and Performance Monitoring

Configuration

SNMP

FortiSIEM uses SNMP to discover the HP BladeSystem and collect hardware statistics. See the instructions on configuring SNMP in your Bladesystem documentation to enable communications with FortiSIEM.

After you have configured SNMP on your BladeSystem blade server, you can configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials in FortiSIEM

See Access Credentials to set access and protocol for SSH, and Telnet.

Cloud Applications

FortiSIEM supports these cloud applications for monitoring.

- Alcide.io KAudit
- AWS Access Key IAM Permissions and IAM Policies
- AWS CloudTrail API
- AWS EC2
- AWS EC2 CloudWatch API
- AWS ELB
- AWS Kinesis
- AWS RDS
- AWS Security Hub
- Box.com
- Cisco Umbrella
- Fortinet FortiCASB
- Google Cloud Platform - Pub/Sub Integration
- Google Workspace (Formerly G Suite and Google Apps)
- Microsoft Azure Audit
- Microsoft Office365 Audit
- Microsoft Cloud App Security
- Microsoft Defender for Identity/Microsoft Azure ATP
- Microsoft Azure Compute
- Microsoft Azure Event Hub
- Microsoft Defender for Endpoint/Microsoft Windows Defender ATP
- Okta
- Salesforce CRM Audit

Alcide.io KAudit

- Integration Points
- Event Types
- Configuration
- Sample Log

Integration Points

Protocol	Information Collected	Used For
Syslog	Audit logs	Security and Compliance Monitoring

Event Types

Go to **RESOURCES > Event Types** and search "AlcideKAudit" in the main content panel **Search...** field.

Configuration

- Configuring Alcide.io to Send Logs
- Configuring FortiSIEM to Receive Logs

Configuring Alcide.io to Send Logs

Follow the steps listed here to send syslog to FortiSIEM.

1. In the **target** section of the ConfigMap, set the following:
   a. Target-type = **syslog**
   b. Syslog host = **<fortisiem.host.com>**
   c. Syslog port = **514**
   d. Syslog-tcp = **false**

Configuring FortiSIEM to Receive Logs

No configuration is needed. FortiSIEM can automatically detect and parse Alcide.io logs based on the built in parser.

Sample Log

```
<109>Feb 28 07:09:18 AlcideKAudit:
{"category":"anomaly","cluster":"devel","etype":"cluster","reasons":[{"values":{"high":
[1]},"doc":"change in count of unique unusual URIs in read access
attempts","period":180000,"direction":"read"}],"time":1582873380000,"short-doc":"change
in targets of access attempts","project":"alcide-rnd","context":{"unusual-uri":
```

```
["LHUt"]},"period":180000,"eid":"cluster","confidence":"high","doc":"unusual change in
count of unique unusual URIs in access attempts","direction":"read"}
```

AWS Access Key IAM Permissions and IAM Policies

To monitor AWS resources in FortiSIEM, an access key and a corresponding secret access key is needed. Prior to the availability of AWS IAM users, the recommendation was to create an access key at the level of root AWS account. This practice has been deprecated since the availability of AWS IAM users as you can read from the AWS Security Credentials best practice guide. If you were monitoring AWS using such access keys, the first step is to delete such keys and create keys based on a standalone IAM user dedicated for monitoring purposes in FortiSIEM. This document explains how to create such a user, and what permissions and policies to add to allow FortiSIEM to monitor your AWS environment.

- Create IAM User for FortiSIEM Monitoring
- Change Permissions for IAM User
- S3 Bucket Read-only Policy

Create IAM User for FortiSIEM Monitoring

1. Login to the IAM Console - Users Tab.
2. Click **Create Users**.
3. Type in a username, e.g. aomonitoring under **Enter User Names**.
4. Leave the checkbox **Generate an access key for each user** selected or select it if it is not selected.
5. Click **Download Credentials** and click on **Close** button.
6. The downloaded CSV file contains the Access Key ID and Secret Access Key that you can use in FortiSIEM to monitor various AWS services. You must add permissions before you can actually add them in FortiSIEM.

Change Permissions for IAM User

1. Select the user you are monitoring.
2. Switch to tab **Permissions**.
3. Click **Attach Policy**.
4. Select *AmazonEC2ReadOnlyAccess, AWSCloudTrailReadOnlyAccess, AmazonRDSReadOnlyAccess, CloudWatchReadOnlyAccess, AmazonSQSFullAccess* and click **Attach Policy**. You can choose to skip attaching some policies if you do not use that service or plan on monitoring that service. For instance, if you do not use RDS, then you do not need to attach *AmazonRDSReadOnlyAccess*.
5. You can choose to provide blanket read-only access to all S3 buckets by attaching the policy *AmazonS3ReadOnlyAccess*. Alternatively, you can specify a more restricted policy as described in the next step.
6. Identify the set of S3 bucket(s) that you have configured to store Cloudtrail logs for each region. You can create an **inline policy**, choose **custom policy**, then paste the sample policy below. Make sure you replace the actual S3 bucket names below *aocloudtrail1, aocloudtrail2* with the ones you have configured.

S3 Bucket Read-only Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"            ],
            "Resource": [
                "arn:aws:s3:::aocloudtrail1",
                "arn:aws:s3:::aocloudtrail2"            ]
        }
    ]
}
```

AWS CloudTrail

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
CloudTrail API	None	None	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Cloudtrail" to see the event types associated with this device. See the Amazon API reference for more information about the event types available for CloudTrail monitoring.

Reports

In **RESOURCES > Reports**, search for "cloudtrail" in the main content panel **Search...** field to see the rules associated with this device.

Configuration

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in AWS Access Key IAM Permissions and IAM Policies.

FortiSIEM receives information about AWS events through the CloudTrail API. After creating an S3 bucket for the storage of log files on AWS, you then configure the Simple Notification Service (SNS) and Simple Queue Service (SQS) to create a notification for the log file and have it delivered by SQS. In your FortiSIEM virtual appliance you then enter access credentials so FortiSIEM can communicate with CloudTrail as it would any other device.

Note: Do not add any extra SNS notifications in the SQS queue. The queue should only have one SNS subscription, otherwise pulling logs will not function.

Create a new CloudTrail

1. Log in to https://console.aws.amazon.com/cloudtrail.
2. Switch to the **region** for which you want to generate cloud trail logs.
3. Click **Trails**.
4. Click on **Add New Trail**.
5. Enter a **Trail name** such as `aocloudtrail`.
6. Select **Yes** for **Apply Trail to all regions**.
   FortiSIEM can pull trails from all regions via a single credential.
7. Select **Yes** for **Create a new S3 bucket**.
8. For S3 bucket, enter a name like s3aocloudtrail.
9. Click **Advanced**.
10. Select **Yes** for **Create a new SNS topic**.
11. For **SNS topic**, enter a name like `snsaocloudtrail`.
12. Leave the rest of advanced settings to the default values.
13. Click **Create**.
    A dialog will confirm that logging is turned on.

Configure Simple Queue Service (SQS) Delivery

1. Log in to https://console.aws.amazon.com/sqs.
2. Switch to the **region** in which you created a new cloudtrail above.
3. Click **Create New Queue**.
4. Enter a **Queue Name** such as `sqsaocloudtrail`.

Setting	Value
Default Visibility Timeout	0 seconds
Message Retention Period This must be set for between 5 and 50 minutes. A lower value is recommended for high event rates to avoid event loss.	10 minutes
Maximum Message Size	256 KB
Delivery Delay	0 seconds
Receive Message Wait Time	5 seconds

5. Click **Create Queue**.
6. When the queue is created, click the **Details** tab and make note of the **ARN** (Amazon Resource Name), as you will need this when configuring the Simple Notification Service below and when configuring the access credentials for FortiSIEM.

Set Up Simple Notification Service (SNS)

1. Log in to https://console.aws.amazon.com/sns.
2. Switch to the **region** where you created the trail and SQS.
3. Select **Topics.**
4. Select the SNS topic `snsaocloudtrail` that you specified when creating a cloudtrail.
5. Click **Actions > Subscribe to topic** from the menu to launch the popup **Create Subscription**.
6. For **Protocol**, select **Amazon SQS**.
7. For **Endpoint**, enter the **ARN** of the queue that you created when setting up SQS.
8. Click **Create Subscription**.

Give Permission for Amazon SNS to Send Messages to SQS

1. Log in to https://console.aws.amazon.com/sqs.
2. Select the queue you created, `sqsaocloudtrail`.
3. In the **Queue Actions** menu, select **Subscribe Queue to SNS Topic**.
4. From the **Choose a Topic** dropdown, select the SNS topic `snsaocloudtrail` that you created earlier.
5. The **Topic ARN** will be automatically filled.
6. Click **Subscribe**.

Note: Ensure that SQS, SNS, S3 bucket and CloudTrail are in the same region.

You do not need to initiate discovery of AWS Cloud Trail, but should check that FortiSIEM is pulling events for AWS by checking for an **amazon.com** entry in **ADMIN > Setup > Pull Events**.

You can configure FortiSIEM to communicate with your device by following the instructions in "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to communicate with the CloudTrail API.

Setting	Value
Name	`aocloudtrail`
Device Type	Amazon AWS CloudTrail
Access Protocol	Amazon AWS CloudTrail
Region	Region where you created the trail.
Bucket	The name of the S3 bucket you created (`s3aocloudtrail`)
SQS Queue URL	Enter the ARN of your queue without the `http://` prefix.

Setting	Value
Password Config	See Password Configuration.
Access Key ID	The access key for your AWS instance.
Secret Key	The secret key for your AWS instance.
Organization	Select an organization from the drop-down list.

Sample Events for AWS CloudTrail

```
Fri Oct 10 14:44:23 2014 FortiSIEM-CloudTrail
[additionalEventData/LoginTo]=https://console.aws.amazon.com/console/home?state=
hashArgs%23&isauthcode=true

[additionalEventData/MFAUsed]=No [additionalEventData/MobileVersion]=No [awsRegion]=us-east-
1 [eventID]=fdf8f837-7e75-46a0-ac95-b6d15993ebf7 [eventName]=ConsoleLogin
[eventSource]=SIGNIN [eventTime]=2014-10-10T06:38:11Z [eventVersion]=1.01
[requestParameters]=null [responseElements/ConsoleLogin]=Success
[sourceIPAddress]=211.144.207.10 [userAgent]=Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.120 Safari/537.36
[userIdentity/accountId]=623885071509
[userIdentity/arn]=arn:aws:iam::623885071509:user/John.Adams
[userIdentity/principalId]=AIDAIUSNMEIUYBS7AN4UW [userIdentity/type]=IAMUser
[userIdentity/userName]=John.Adams

Fri Oct 10 14:19:45 2014 FortiSIEM-CloudTrail [awsRegion]=us-east-1 [eventID]=351bda80-39d4-
41ed-9e4d-86d6470c2436 [eventName]=DescribeInstances [eventSource]=EC2 [eventTime]=2014-10-
10T06:12:24Z [eventVersion]=1.01 [requestID]=2d835ae2-176d-4ea2-8523-b1a09585e803
[requestParameters/filterSet/items/0/name]=private-ip-address
[requestParameters/filterSet/items/0/valueSet/items/0/value]=10.0.0.233
[responseElements]=null [sourceIPAddress]=211.144.207.10 [userAgent]=aws-sdk-php2/2.4.7
Guzzle/3.7.1 curl/7.19.7 PHP/5.3.3 [userIdentity/accessKeyId]=AKIAI2MUUCROHFSLLT3A
[userIdentity/accountId]=623885071509 [userIdentity/arn]=arn:aws:iam::623885071509:root
[userIdentity/principalId]=623885071509 [userIdentity/type]=Root
[userIdentity/userName]=accelops
```

Performance Tuning for High EPS CloudTrail Events

AWS CloudTrail can generate a lot of events. Follow these recommendations to enable FortiSIEM to keep up with high EPS CloudTrail events.

1. In the AWS configuration, change the **Message retention period** of SQS to 1 day.
2. Adjust the `CloudTrail` event pulling parameters as follows. Go to the Collector that pulls AWS CloudTrail events. You will find these three relevant parameters in the `/opt/phoenix/config/phoenix_config.txt` file:
   - `cloudtrail_msg_pull_interval` (default 30 seconds, minimum recommended 10 seconds) - how often CloudTrail events are pulled.
   - `cloudtrail_msg_pull_thread_num` (default 1, maximum recommended 60) - how many threads are used to pull CloudTrail events.
   - `cloudtrail_file_parse_thread_num` (default 3, maximum recommended 60) - how many threads are used to parse CloudTrail events.

Since each API call returns maximum 10 files, set the parameters to satisfy the following two constraints. If the thread count is high, then you must increase the number of vCPUs in the Collector.

- Set (`SQSInputEventRate` times `cloudtrail_msg_pull_interval`) to be smaller than (`cloudtrail_msg_pull_thread_num` times 10)
- Set `cloudtrail_msg_pull_thread_num` to be equal to `cloudtrail_file_parse_thread_num`

Amazon AWS EC2

- Configuration

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	<set name>
Device Type	Amazon AWS EC2
Access Protocol	AWS SDK
Region	[Required] Region in which your AWS instance is located
Access Key ID	[Required] Access key for your AWS instance
Secret Key	[Required] Secret key for your AWS instance
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Amazon AWS EC2.
5. To see the jobs associated with AWS, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "AWS" in the search box.

AWS EC2 CloudWatch API

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Amazon

Product Information: https://aws.amazon.com/cloudwatch/

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
CloudWatch API	• Machine name • Internal Access IP • Instance ID • Image ID • Availability Zone • Instance Type • Volume ID • Status • Attach Time • Event Logs	• CPU Utilization • Received Bits/sec • Sent Bits/sec • Disk reads (Instance Store) • Disk writes (Instance Store) • Disk reads/sec (Instance Store) • Disk writes/sec (Instance Store) • Packet loss • Read Bytes (EBS) • Write Bytes (EBS) • Read Ops (EBS) • Write Ops (EBS) • Disk Queue (EBS) • AWS or Custom event logs stored in AWS CloudWatch	Performance Monitoring CloudWatch Events Monitoring

Event Types

- PH_DEV_MON_EBS_METRIC captures EBS metrics

In **ADMIN > Device Support > Event Types**, search for "AWS-CloudTrail" to see the event types associated with this device. CloudWatch allows for different AWS event sources and custom event sources to store events in AWS CloudTrail.

To search for these event types, from **ANALYTICS**, click in the **Edit Filters and Time Range...** field, and take the following steps:

1. In Filter, select the **Event Attribute** radio button.
2. In the **Attribute** field, enter "Event Type".
3. In the **Operator** field, select "CONTAIN".
4. In the **Value** field, enter "AWS_VPC_FLOW".
5. Under **Row**, click **+** to add another row.
6. In the new row, in the **Attribute** field, enter "Raw Event Log".
7. In the new row, in the **Operator** field, select "CONTAIN".
8. In the new row, in the **Value** field, enter "AWS_CLOUDWATCH_EVENT_DATA".
9. Configure your Time Range and click **Apply & Run**.

Configuration

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in AWS Access Key IAM Permissions and IAM Policies.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide. You should also be sure to read the topic "Discovering Amazon Web Services (AWS) Infrastructure".

VPC Flow logs are supported. For more information, see HOW TO - Integrate Amazon VPC Flows.

The purpose of this discovery is to poll a list of EC2 instances in a given region so FortiSIEM knows that they are part of your AWS infrastructure. No logs are collected, but a CMDB entry for each EC2 instance is categorized under the “AWS” group in CMDB. This is important for certain reports that only look at AWS resources. It is still required to configure individual VMs with appropriate logging configurations, such as installable Agents (Linux, Windows) or Agentless (Syslog or WMI). Follow the instructions for the type of guest VM in this guide.

If you only want CloudWatch integration, you can create your AWS user and configure that user's policy by taking these steps.
Note: For the latest AWS documentation, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Users** and then choose **Add user**.
3. Type the user name for the new user. This is the sign-in name for AWS.
4. Select **Programmatic access** for the type of access this user will have.
5. Choose **Next: Permissions**.
6. Select **Attach existing policies directly**.
7. Select the policy **CloudwatchReadOnlyAccess**.
8. Choose **Next: Tags**.
9. Choose **Next: Review**.
10. Choose **Create user**.
11. Choose **Show** and record the Access key ID.

    Note: To save the access keys, choose **Download .csv** and then save the file to a safe location.

This is your only opportunity to view or download the secret access keys. You will not have access to the secret keys again after this step.

12. Choose **Show** and record the secret key.

    Note: To save the access keys, choose **Download .csv** and then save the file to a safe location.

    This is your only opportunity to view or download the secret access keys. You will not have access to the secret keys again after this step.
13. Click **Close**.

Settings for Access Credentials

FortiSIEM Configuration Setup

Complete these steps in the FortiSIEM UI:

1. Navigate to **ADMIN > Setup** and click the **Credentials** tab.
2. In **Step 1: Enter Credentials**:
    a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
    b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Setting	Value
Name	ec2
Device Type	Amazon AWS CloudWatch
Access Protocol	AWS CloudWatch
Region	The region in which your AWS instance is located
AWS Account	The name of your AWS account.
Log Group Name	Name of the log group.
Log Stream Name	Name of the log stream.
Password Config	See Password Configuration.
Access Key ID	The access key for your EC2 instance
Secret Key	The secret key for your EC2 instance

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
    a. Select the ec2 credential you created earlier from the **Credentials** drop-down list. It should autofill **IP/Host Name** as destination "amazon.com".
    b. Click **Save**.
4. Select the new mapping and click the **Test** drop-down list and select **Test Connectivity without Ping** to start pulling.

Sample Events

```
[PH_DEV_MON_EC2_METRIC]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=6571,[hostName]=ec2-54-81-216-218.compute-1.amazonaws.com,
[hostIpAddr]=10.144.18.131,[cpuUtil]=0.334000,[diskReadKBytesPerSec]=0.000000,
[diskWriteKBytesPerSec]=0.000000,[diskReadReqPerSec]=0.000000,[diskWriteReqPerSec]=0.000000,
[sentBytes]=131,[recvBytes]=165,[sentBitsPerSec]=17.493333,[recvBitsPerSec]=22.026667,
[phLogDetail]=
```

```
[PH_DEV_MON_EBS_METRIC]:[eventSeverity]=PHL_INFO,[fileName]=deviceAws.cpp,
```

```
[lineNumber]=133,[hostName]=ec2-52-69-215-178.ap-northeast-1.compute.amazonaws.com,
[hostIpAddr]=172.30.0.50,[diskName]=/dev/sda1,[volumeId]=vol-63287d9f,
[diskReadKBytesPerSec]=7.395556,[diskWriteKBytesPerSec]=7.395556,[ioReadsPerSec]=0.000000,
[ioWritesPerSec]=0.010000,[diskQLen]=0,[phLogDetail]=
```

AWS Elastic Load Balancer (ELB)

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Event

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
AWS API		Permitted traffic	Log analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "aws elb" to see the event types associated with this device.

Rules

There are no specific rules available for AWS ELB.

Reports

In **RESOURCES > Reports**, search for "aws elb" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- Setup in AWS
- Setup in FortiSIEM

Setup in AWS

Follow the steps here to complete your setup in AWS.

- Enable Elastic Load Balancing Access Logs
- Enable Event Notifications
- Generate a New Access Key

Enable Elastic Load Balancing Access Logs

Take the following steps to enable Elastic Load Balancing Access Logs.

1. Go to the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. On the navigation pane, under **LOAD BALANCING**, select **Load Balancers**.
3. Select your load balancer.
4. On the **Description** tab, select **Configure Access Logs**.
5. On the **Configure Access Logs** page, take the following steps:
   a. Select **Enable access logs**.
   b. Leave **Interval** as the default (60 minutes).
   c. At **S3 location**, enter the name of your S3 bucket, including the prefix, for example, `my-loadbalancer-logs/my-app`. You can specify the name of an existing bucket or a name for a new bucket.
   d. (Optional) If the bucket does not exist, select **Create this location for me**. You must specify a name that is unique across all existing bucket names in Amazon S3 and follows the DNS naming conventions. For more information, see Bucket naming rules in the Amazon Simple Storage Service Guide.
   e. Click **Save**.

Enable Event Notifications

Take the following steps to enable Event Notifications.

1. Go to the Amazon S3 console at https://s3.console.aws.amazon.com/s3/.
2. Select your bucket.
3. Click **Properties**.
4. Click **Event notifications > Create event notification**.
   a. Input **Event name** and **Prefix**.
   b. Select **All object create events for Event Types**.
   c. Select **SQS queue** for **Destination**.
   d. Select your SQS.
   e. Click **Save changes**.

   Notes:

   - There are no other servers to use with SQS. This is because the format of the message in SQS coming from other servers may not be the same as that coming from S3 used by the ELB server. For example, a message coming from the Cloudtrail server may not be the same.
   - Ensure the **Message retention period** property for SQS is 12 hours.
   - Ensure the **Default visibility timeout** property for SQS is 1 day.

Generate a New Access Key

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, select **Users**.
3. Click **Add user**.
4. In the **User Name** field, enter a user name.
5. For **AWS access type**, select **Programmatic access**.
6. Click **Next: Permissions**.

7. Select the **Attach existing policies directly** tab.
8. Select **AmazonS3ReadOnlyAccess** and **AmazonSQSFullAccess**.
9. Click **Next: Tags**, then click **Next: Review**.
10. Click **Create user**.
11. Click **Download Credentials**. The downloaded CSV file contains the Access Key ID and Secret Access Key that will be used in FortiSIEM.
12. Click **Close**.

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in AWS Access Key IAM Permissions and IAM Policies.

You can now configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide. You should also be sure to read the topic Discovering Amazon Web Services (AWS) Infrastructure.

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:
   Note: Make sure no other devices use the same credential, otherwise events may appear missing.

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS ELB
Access Protocol	AWS_ELB
Region	The region in which your AWS instance is located
Bucket	The AWS S3 bucket
SQS Queue URL	Provide the full URL, for example: `https://sqs.us-west-2.amazonaws.com/623885071509/sqsforloadblancer`
Password Config	See Password Configuration.
Access Key ID	The access key for your EC2 instance
Secret Key	The secret key for your EC2 instance

Settings	Description
Confirm Secret Key	Enter the secret key for validation.
Session Token	If you provided an access key, you can leave this field blank.
Organization	Select an organization from the drop-down list.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS ELB.
5. To see the jobs associated with AWS ELB, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "ELB" in the search box.

Sample Event

```
AWS-ELB:phCustId=1,reptDevIpAddr=10.10.103.205,reptDevName=amazon.com,msg=http 2021-02-
11T01:56:06.000372Z app/shashi-elb/061d492a88a60fb1 10.10.168.108:46938 - -1 -1 -1 503 - 500
337 "POST http://10.10.29.144:80/boaform/admin/formLogin HTTP/1.1" "Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0" - -
arn:aws:elasticloadbalancing:us-west-2:623885071509:targetgroup/shashi-tg/974fbb8764192573
"Root=1-60248eb5-01950dcf187ac3c244ab2231" "-" "-" 0 2021-02-11T01:56:05.999000Z "forward"
"-" "-" "-" "-" "-" "-"
```

AWS Kinesis

Amazon Kinesis is an Amazon Web Service (AWS) for processing big data in real time. Kinesis is capable of processing hundreds of terabytes per hour from high volumes of streaming data from sources such as operating logs, financial transactions and social media feeds.

What is Discovered and Monitored

Protocol	Information collected	Used for
Amazon AWS Client Library	Streaming data	Collect, process, and analyze real-time streaming data.

Event Types

In **RESOURCES > Event Types**, enter "Kinesis" in the main content panel **Search...** field to see the event types associated with this device.

Rules

No defined rules.

Reports

No defined reports.

Configuring AWS Kinesis

1. Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the IAM console.
2. In the navigation bar on the upper right, choose your user name, and then choose My Security Credentials.
3. On the AWS **IAM Credentials** tab, in the Access keys for CLI, SDK, and API access section, do any of the following:

- To create an access key, choose **Create access key**. Then choose **Download .csv** file to save the access key ID and secret access key to a .csv file on your computer. Store the file in a secure location. You will not have access to the secret access key again after this dialog box closes. After you have downloaded the .csv file, choose **Close**. When you create an access key, the key pair is active by default, and you can use the pair right away.
- To disable an active access key, choose **Make inactive**.
- To reenable an inactive access key, choose **Make active**.
- To delete an access key, choose its **X** button at the far right of the row. Then choose **Delete** to confirm. When you delete an access key, it's gone forever and cannot be retrieved. However, you can always create new keys.

Configuring FortiSIEM

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS Kinesis
Access Protocol	AWS Kinesis Client Library
Region	You can enter one or more regions separated by a space, for example, "us-east-1 us-west-2". See Supported Regions in AWS for a list of valid regions.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration. For CyberArk REST API, see CyberArk REST API Password Configuration. For RAX_Janus, see RAX_Janus Password Configuration.
Access Key	Access key for your AWS Kinesis instance. See Configuring AWS Kinesis.
Secret Key	Secret key for your AWS Security Hub instance
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your AWS Kinesis credential from the **Credentials** drop-down list.

   c. Click **Save**.

4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS Kinesis.
5. To see the jobs associated with AWS Kinesis, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "AWS Kinesis" in the search box.

Configuring AWS CloudTrail Logs through Kinesis Streams

The data flow for this setup is AWS CloudTrail -> AWS CloudWatch -> AWS Kinesis Data Streams.

Taking the following steps to configure.

Prerequisite

- Obtain your access key and secret for a user account with administrator privileges.
- Ensure the AWS CLI is installed. Fore more information on AWS CLI, see here.

1. Run from cmd:

   ```
   aws configure
   ```

   Enter your access key, secret and default region.

   Example:

   ```
   Account ID: 11111111111
   Access Key ID: aaaaaaaaaaaaaaaaaaaaa
   Access Secret: 13452322222222222222
   Region: us-west-1
   Kinesis Role: SIEMKinesisRole
   ```

   Note: This will be created in a later portion of this guide.
2. Create log group by entering the following:

   ```
   aws logs create-log-group --log-group-name "cloudwatch-group"
   aws logs describe-log-groups
   ```
3. Create a cloudtrail role that permits sending logs to the CloudWatch log group by putting the following JSON into a file, and save it as a JSON file on your desktop.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "",
         "Effect": "Allow",
         "Principal": {
           "Service": "cloudtrail.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
       }
     ]
   }
   ```
4. Use the AWS CLI to run the following command, referencing the file path where you saved the JSON file. In this command example, the file above was saved as `cloudtrail-role.json`.

   ```
   aws iam create-role --role-name CTRole --assume-role-policy-document
   file://cloudtrail-role.json
   ```

5. Create the CloudTrail policy-document by saving the following JSON into a file, saving it to your desktop.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-west-1:11111111111:log-group:CloudTrail:log-stream:11111111111_
CloudTrail_us-west-1*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-west-1:11111111111:log-group:CloudTrail:log-stream:11111111111_
CloudTrail_us-west-1*"
      ]
    }
  ]
}
```

6. Use the AWS CLI to run the following command, referencing the file path where you saved the JSON file. In this command example, the file above was saved as `cloudtrail-policy.json`. **Note**: What we're doing here is creating a role called “CTRole” and applying a policy to it.

```
aws iam put-role-policy --role-name CTRole --policy-name cloudtrail-policy --
policy-document file://cloudtrail-policy.json
```

Kinesis Configuration Setup

Take the following steps to configure Kinesis. **Note**: The latest instructions can be found here.

1. Create an AWS Kinesis stream (if it does not exist). In this example, we'll create one called "fortisiem".

```
aws kinesis create-stream --stream-name "fortisiem"
```

2. Create a file called "TrustPolicyForCWL.json" using the following code.

```
{
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "logs.us-west-1.amazonaws.com" },
    "Action": "sts:AssumeRole"
  }
}
```

3. Create an iam role with the defined policy, called "CWLtoKinesisRole" by running the following command.

   ```
   aws iam create-role --role-name CWLtoKinesisRole --assume-role-policy-document
   file://~/TrustPolicyForCWL.json
   ```

4. Create a permission file called "PermissionsForCWL.json" using the following code.

   ```
   {
     "Statement": [
       {
         "Effect": "Allow",
         "Action": "kinesis:PutRecord",
         "Resource": "arn:aws:kinesis:us-west-1: 111111111111:stream/fortisiem"
       }
     ]
   }
   ```

5. Associate the above policy file with the role we created, by running the following command.

   ```
   aws iam put-role-policy --role-name CWLtoKinesisRole --policy-name Permissions-
   Policy-For-CWL --policy-document
   ```

6. Create the subscription to forward cloudwatch logs.

   Note: The following multiline command is for Windows, as ^ indicates the command continues on the next line. If using Linux, use the multiline command for Linux, which replaces the ^ with \. Paste all of it in as one command.

   Windows:

   ```
   //Create  CloudWatch Log Susbscription filter:
   aws logs put-subscription-filter ^
       --log-group-name "cloudwatch-group" ^
       --filter-name "fortisiem" ^
       --filter-pattern "" ^
       --destination-arn "arn:aws:kinesis:us-west-1:111111111111:stream/fortisiem " ^
       --role-arn "arn:aws:iam::111111111111:role/CWLtoKinesisRole "
   ```

   Linux:

   ```
   //Create  CloudWatch Log Susbscription filter:
   aws logs put-subscription-filter \
       --log-group-name "cloudwatch-group" \
       --filter-name "fortisiem" \
       --filter-pattern "" \
       --destination-arn "arn:aws:kinesis:us-west-1:111111111111:stream/fortisiem " \
       --role-arn "arn:aws:iam::111111111111:role/CWLtoKinesisRole "
   ```

7. Create an IAM user account that FortiSIEM can use to ingest Kinesis Data Streams. When assigning permissions for the IAM user, the following must be allowed.

Consumer		
Actions	**Resource**	**Purpose**
DescribeStream	Kinesis data stream	Before attempting to read records, the consumer checks if the stream exists and is active, and if the shards are contained in the stream.

Consumer Actions	Resource	Purpose
Get Records, Get ShardIterator	Kinesis data stream	Read records from a Kinesis Data Streams shard.
CreateTable, DescribeTable, GetItem, PutItem, Scan, Update Item	Amazon DynamoDB table	If the consumer is developed using the Kinesis Client Library (KCL), it needs permissions to a DynamoDB table to track the processing state of the application. The first consumer started creates the table.
Delete Item	Amazon DynamoDB table	For when the consumder performs split/merge operations on Kinesis Data Stream shards.
PutMetricData	Amazon CloudWatch log	The KCL also uploads metrics to CloudWatch, which are useful for monitoring the application.

8. Navigate to IAM -> Users -> Add user
   Access Type: Programmatic Access
   Next Permission:
9. Under permissions, select Attach existing policies directly
   AmazonKinesisReadOnlyAccess
   AmazonDynamoDBFullAccess
   CloudWatchLogsFullAccess
   Note: If step 11 is followed, it replaces the more generic access policy set here in step 9, which would no longer be needed.
10. Click Next -> Review.
    You should see that under Permissions summary, the following policies attached to the user.

Type	Name
Managed policy	CloudWatchLogsFullAccess
Managed policy	AmazonDynamoDBFullAccess
Managed policy	AmazonKinesisReadOnlyAccess

11. Once the user is created, generate an access key and secret for this user. The following reference link demonstrates how to implement restrictive, minimum access policies to FortiSIEM (which is the consumer as referenced in the guide). - https://docs.aws.amazon.com/streams/latest/dev/tutorial-stock-data-kplkcl-iam.html
Note: For advanced users, you can customize permissions policies to allow only access to a specific CloudWatch log group, specific Kinesis Stream, etc....

FortiSIEM Configuration Setup

Go to the **ADMIN > Setup > Credentials** tab.

In **Step 1: Enter Credentials**:

1. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
2. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, such as KinesisStreamIntegration
Device Type	Amazon AWS Kinesis
Access Protocol	AWS Kinesis Client Library
Region	You can enter one or more regions separated by a space, for example, “us-east-2 us-west-1”. See Supported Regions in AWS for a list of valid regions.
Log Stream Name	Enter "fortisiem" or the name of your stream.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration. For CyberArk REST API, see CyberArk REST API Password Configuration. For RAX_Janus, see RAX_Janus Password Configuration.
Access Key	Access key for your AWS Kinesis instance. See Configuring AWS Kinesis.
Secret Key	Your Secret key.
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, to the right of the **Search...** field, select the desired collector that will poll CloudTrail logs from the drop-down list if you have more than one collector. If only one collector is available, the drop-down list will not be available.
4. Click **New**.
   a. Select the CloudTrail credential you created earlier from the **Credentials** drop-down list. It should autofill **IP/Host Name** as destination "amazon.com". FortiSIEM will handle communication to the appropriate API.

   b. Click **Save**.

5. Select the new mapping and click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling.
6. To see the jobs associated with AWS Kinesis, select **ADMIN > Setup > Pull Events**.
7. To see the received events select **ANALYTICS**, then enter "AWS Kinesis" in the search box.

Configuring VPC Flow Logs through Kinesis Streams

The data flow for this setup is AWS VPC Flow Logs -> AWS CloudWatch -> AWS Kinesis Data Streams.

Taking the following steps to configure.

Prerequisite

- Obtain your access key and secret for a user account with administrator privileges.
- Ensure the AWS CLI is installed. Fore more information on AWS CLI, see here.

1. Run from cmd:
   ```
   aws configure
   ```
   Enter your access key, secret and default region.

   Example:
   ```
   Account ID: 11111111111

   Access Key ID: aaaaaaaaaaaaaaaaaaaaa

   Access Secret: 1345232222222222222

   Region: us-west-1
   ```
2. Configure AWS VPC flow logs to send to CloudWatch logs by following similar steps documented here.

Kinesis Configuration Setup

Take the following steps to configure Kinesis. **Note**: The latest instructions can be found here.

1. Create an AWS Kinesis stream (if it does not exist). In this example, we'll create one called "fortisiem".
   ```
   aws kinesis create-stream --stream-name "fortisiem"
   ```
2. Create a file called "TrustPolicyForCWL.json" using the following code.
   ```
   {
     "Statement": {
       "Effect": "Allow",
       "Principal": { "Service": "logs.us-west-1.amazonaws.com" },
       "Action": "sts:AssumeRole"
     }
   }
   ```
3. Create an iam role with the defined policy, called "CWLtoKinesisRole" by running the following command.
   ```
   aws iam create-role --role-name CWLtoKinesisRole --assume-role-policy-document
   file://~/TrustPolicyForCWL.json
   ```
4. Create a permission file called "PermissionsForCWL.json" using the following code.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kinesis:PutRecord",
      "Resource": "arn:aws:kinesis:us-west-1: 11111111111:stream/fortisiem"
    }
  ]
}
```

5. Associate the above policy file with the role we created, by running the following command.

   ```
   aws iam put-role-policy --role-name CWLtoKinesisRole --policy-name Permissions-
   Policy-For-CWL --policy-document
   ```

6. Create the subscription to forward cloudwatch logs.

   Note: The following multiline command is for Windows, as ^ indicates the command continues on the next line. If using Linux, use the multiline command for Linux, which replaces the ^ with \. Paste all of it in as one command.

   Windows:

   ```
   //Create  CloudWatch Log Susbscription filter:
   aws logs put-subscription-filter ^
       --log-group-name "cloudwatch-group" ^
       --filter-name "fortisiem" ^
       --filter-pattern "" ^
       --destination-arn "arn:aws:kinesis:us-west-1:11111111111:stream/fortisiem " ^
       --role-arn "arn:aws:iam::11111111111:role/CWLtoKinesisRole "
   ```

   Linux:

   ```
   //Create  CloudWatch Log Susbscription filter:
   aws logs put-subscription-filter \
       --log-group-name "cloudwatch-group" \
       --filter-name "fortisiem" \
       --filter-pattern "" \
       --destination-arn "arn:aws:kinesis:us-west-1:11111111111:stream/fortisiem " \
       --role-arn "arn:aws:iam::11111111111:role/CWLtoKinesisRole "
   ```

7. Create an IAM user account that FortiSIEM can use to ingest Kinesis Data Streams. When assigning permissions for the IAM user, the following must be allowed.

Consumer Actions	Resource	Purpose
DescribeStream	Kinesis data stream	Before attempting to read records, the consumer checks if the stream exists and is active, and if the shards are contained in the stream.
Get Records, Get ShardIterator	Kinesis data stream	Read records from a Kinesis Data Streams shard.

Consumer		
Actions	**Resource**	**Purpose**
CreateTable, DescribeTable, GetItem, PutItem, Scan, Update Item	Amazon DynamoDB table	If the consumer is developed using the Kinesis Client Library (KCL), it needs permissions to a DynamoDB table to track the processing state of the application. The first consumer started creates the table.
Delete Item	Amazon DynamoDB table	For when the consumder performs split/merge operations on Kinesis Data Stream shards.
PutMetricData	Amazon CloudWatch log	The KCL also uploads metrics to CloudWatch, which are useful for monitoring the application.

8. Navigate to IAM -> Users -> Add user
   Access Type: Programmatic Access
   Next Permission:
9. Under permissions, select Attach existing policies directly
   AmazonKinesisReadOnlyAccess
   AmazonDynamoDBFullAccess
   CloudWatchLogsFullAccess
   Note: If step 11 is followed, it replaces the more generic access policy set here in step 9, which would no longer be needed.
10. Click Next -> Review.
    You should see that under Permissions summary, the following policies attached to the user.

Type	Name
Managed policy	CloudWatchLogsFullAccess
Managed policy	AmazonDynamoDBFullAccess
Managed policy	AmazonKinesisReadOnlyAccess

11. Once the user is created, generate an access key and secret for this user. The following reference link demonstrates how to implement restrictive, minimum access policies to FortiSIEM (which is the consumer as referenced in the guide). - https://docs.aws.amazon.com/streams/latest/dev/tutorial-stock-data-kplkcl-iam.html
    Note: For advanced users, you can customize permissions policies to allow only access to a specific CloudWatch

log group, specific Kinesis Stream, etc....

FortiSIEM Configuration Setup

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, such as KinesisStreamIntegration
Device Type	Amazon AWS Kinesis
Access Protocol	AWS Kinesis Client Library
Region	You can enter one or more regions separated by a space, for example, “us-east-2 us-west-1”. See Supported Regions in AWS for a list of valid regions.
Log Stream Name	Enter "fortisiem" or the name of your stream.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration. For CyberArk REST API, see CyberArk REST API Password Configuration. For RAX_Janus, see RAX_Janus Password Configuration.
Access Key	Access key for your AWS Kinesis instance. See Configuring AWS Kinesis.
Secret Key	Your Secret key.
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, to the right of the **Search...** field, select the desired collector that will poll CloudTrail logs from the drop-down list if you have more than one collector. If only one collector is available, the drop-down list will not be available.
4. Click **New**.
   a. Select the CloudTrail credential you created earlier from the **Credentials** drop-down list. It should autofill the **IP/Host Name** field as destination "amazon.com". FortiSIEM will handle communication to the appropriate API.
   b. Click **Save**.
5. Click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling.

6. To see the jobs associated with AWS Kinesis, select **ADMIN > Setup > Pull Events**.
7. To see the received events select **ANALYTICS**, then enter "AWS Kinesis" in the search box.

Sample Events

VPC Log Example

```
2021-04-27T08:40:50.00Z [FSM-AWSKinesis] 2 311111777194 eni-054c755e644dcf32d 103.114.104.68
172.31.9.216 22898 22717 6 1 40 1619538050 1619538102 REJECT OK

2021-04-27T09:14:45.00Z [FSM-AWSKinesis] 2 311111777194 eni-054c755e644dcf32d 172.31.9.216
222.187.239.109 22 43638 6 3 3996 1619540085 1619540142 ACCEPT OK
```

CloudTrail Log Example

```
2021-04-28T14:29:51.783Z [FSM-AWSKinesis] {"eventVersion":"1.08","userIdentity":
{"type":"Root","principalId":"921045424829","arn":"arn:aws:iam::1234567890AB:root","accountI
d":"111115424829","accessKeyId":"ASIA1234567890ABCDEF","sessionContext":{"sessionIssuer":
{},"webIdFederationData":{},"attributes":{"mfaAuthenticated":"false","creationDate":"2021-
04-28T20:37:47Z"}}},"eventTime":"2021-04-
28T21:13:07Z","eventSource":"health.amazonaws.com","eventName":"DescribeEventAggregates","aw
sRegion":"us-east-
1","sourceIPAddress":"10.20.30.40","userAgent":"console.amazonaws.com","requestParameters":
{"aggregateField":"eventTypeCategory","filter":{"eventStatusCodes":
["open","upcoming"],"startTimes":[{"from":"Apr 21, 2021 9:13:07
PM"}]}},"responseElements":null,"requestID":"1a712381-62d1-4485-8ce5-
109930945c62","eventID":"eb8c077f-321d-471a-b207-
849f5089a428","readOnly":true,"eventType":"AwsApiCall","managementEvent":true,"eventCategory
":"Management","recipientAccountId":"921045424829"}
```

AWS RDS

- What is Discovered and Monitored
- Event Types
- Configuration
- Sample Events

What is Discovered and Monitored

Type	Protocol	Information Discovered	Metrics Collected	Used For
Relational Database Storage (RDS)	CloudWatch API		• CPU Utilization • User Connections • Free Memory • Free Storage • Used Swap • Read Latency • Write Latency • Read Ops • Write Ops	Performance Monitoring

Event Types

- PH_DEV_MON_RDS_METRIC captures RDS metrics

Configuration

If you have not already configured Access Keys and permissions in AWS, please follow the steps outlined in AWS Access Key IAM Permissions and IAM Policies.

Discovering AWS RDS

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS RDS

Settings	Description
Access Protocol	AWS SDK
Region	Set **Region** as the region in which your AWS instance is located.
Password Config	See Password Configuration.
Access Key ID	Access key for your EC2 instance.
Secret Key	Secret key for your EC2 instance
Organization	Select an **Organization** from the drop-down list.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Set **IP/Host Name** to amazon.com.
   b. Select the name of your AWS RDS credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS RDS.
5. Go to **ADMIN > Setup > Discovery**.
6. Click **New**.
7. Fill out the information in the Discovery Definition window, ensuring you set **Discovery Type** as AWS Scan.
8. When done, click **Save**.
9. Select the entry and click **Discover**.
10. After Discovery finishes, check **CMDB > Devices > Amazon Web Services > AWS Database**.

Sample Events

```
[PH_DEV_MON_RDS_METRIC]:[eventSeverity]=PHL_INFO,[fileName]=deviceAwsRDS.cpp,
[lineNumber]=104,[hostName]=mysql1.cmdzvvce07ar.ap-northeast-1.rds.amazonaws.com,
[hostIpAddr]=54.64.131.93,[dbCpuTimeRatio]=1.207500,[dbUserConn]=0,
[dbEnqueueDeadlocksPerSec]=0.000587,[freeMemKB]=489,[freeDiskMB]=4555,
[swapMemUtil]=0.000000,[ioReadsPerSec]=0.219985,[ioWritesPerSec]=0.213329,
[devDiskRdLatency]=0.08,[devDiskWrLatency]=0.4029,[phLogDetail]=
```

AWS Security Hub

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Requirements
- Configuring AWS Security Hub
- To Create, Modify, or Delete Your Own IAM User Access Keys (Console)
- Configuring FortiSIEM for AWS Security Hub Access
- Sample Events

Security Hub collects security data from across AWS accounts, services, and supported third-party partner products. Configure FortiSIEM to gather this data collected by Security Hub, so FortiSIEM can analyze this data to identify the highest priority security issues.

What is Discovered and Monitored

Protocol	Information collected	Used for
AWS Security Hub SDK	Security data	Security and compliance

Event Types

In **RESOURCES > Event Types**, enter "AWS Sechub" in the main content panel **Search...** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, enter "AWS Sechub" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, enter "AWS Security Hub" in the main content panel **Search...** field to see the reports associated with this device.

Requirements

FortiSIEM uses PHP V3 SDK to integrate data from the security hub to perform comprehensive security analytics.

Configuring AWS Security Hub

Supported Regions in AWS

Security Hub only collects events from the region where you enabled Security Hub. If you don't enable the Security Hub for other regions, then you won't get events from those regions. FortiSIEM allows you to specify multiple regions when you create a new credential. In the regions you specify, the Security Hub will be enabled. These regions should use the following AWS region codes:

Region Name	Region Code
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
EU (Stockholm)	eu-north-1
South America (São Paulo)	sa-east-1

Step 1: Enable Security Hub

Permissions required to enable Security Hub

1. The IAM identity (user, role, or group) that you use to enable Security Hub must have the required permissions. To grant the permissions required to enable Security Hub, attach the following policy to an IAM user, group, or role.
   ```
   {
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
   "Action": "securityhub:*",
   "Resource": "*"
   },
   {
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "*",
   "Condition": {
   "StringLike": {
   "iam:AWSServiceName": "securityhub.amazonaws.com"
   }
   }
   }
   ]
   }
   ```
2. Use the credentials of the IAM identity from step 1 to sign in to the Security Hub console. When you open the Security Hub console for the first time, choose **Get Started** and then choose **Enable Security Hub**.

Step 2: Get an Access Key

This feature supports long-term access keys. Access keys consist of two parts: an access key ID and a secret access key.

Permissions Required

To create access keys for your own IAM user, you must have the permissions from the following policy:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "CreateOwnAccessKeys",
"Effect": "Allow",
```

```
"Action": [
"iam:CreateAccessKey",
"iam:GetUser",
"iam:ListAccessKeys"
],
"Resource": "arn:aws:iam::*:user/${aws:username}"
}
]
}
```

To Create, Modify, or Delete Your Own IAM User Access Keys (Console)

1. Use your AWS account ID or account alias, your IAM user name, and your password to sign in to the IAM console.
2. In the navigation bar on the upper right, choose your user name, and then choose My Security Credentials.
3. On the AWS IAM Credentials tab, in the Access keys for CLI, SDK, and API access section, do any of the following:
   - To create an access key, choose Create access key. Then choose Download .csv file to save the access key ID and secret access key to a .csv file on your computer. Store the file in a secure location. You will not have access to the secret access key again after this dialog box closes. After you have downloaded the .csv file, choose Close. When you create an access key, the key pair is active by default, and you can use the pair right away.
   - To disable an active access key, choose Make inactive.
   - To reenable an inactive access key, choose Make active.
   - To delete an access key, choose its X button at the far right of the row. Then choose Delete to confirm. When you delete an access key, it's gone forever and cannot be retrieved. However, you can always create new keys.

Configuring FortiSIEM for AWS Security Hub Access

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Amazon AWS Security Hub
Access Protocol	AWS Security Hub SDK
Region	You can enter one or more regions separated by a space, for example, “us-

Settings	Description
	east-1 us-west-2”. See Supported Regions in AWS for a list of valid regions.
Password Config	Choose Manual, CyberArk SDK, CyberArk REST API, or RAX_Janus from the drop down list. For CyberArk SDK, see CyberArk SDK Password Configuration. For CyberArk REST API, see CyberArk REST API Password Configuration. For RAX_Janus, see RAX_Janus Password Configuration.
Access Key	Access key for your AWS Security Hub instance. See Step 2: Get an Access Key.
Secret Key	Secret key for your AWS Security Hub instance
Session Token	The session token is used by credentials from Rax Scan. If you obtained an access key as described in Step 2: Get an Access Key, then leave this field empty.
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Select the name of your AWS Security Hub credential from the **Credentials** drop-down list. The **IP/Host Name** field/destination should auto populate to "amazon.com".
   b. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to AWS Security Hub.
5. To see the jobs associated with AWS Security Hub, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "AWS Security Hub" in the search box.

Sample Events

```
[AWS_SECURITY_HUB_EVENT_DATA] ={
 "AwsAccountId": "111111111111",
 "CreatedAt": "2019-08-06T04:56:44.894Z",
 "Description": "10.10.10.72 is performing SSH brute force attacks against i-
0100ee1e110c011c1. Brute force attacks are used to gain unauthorized access to your instance
by guessing the SSH password.",
 "FirstObservedAt": "2019-08-06T04:51:14Z",
 "GeneratorId": "arn:aws:guardduty:us-west-
2:111111111111:detector/50b2ea07131dbe1530c23facb594b1fa",
 "Id": "arn:aws:guardduty:us-west-
2:111111111111:detector/50b2ea07131dbe1530c23facb594b1fa/finding/8cb632a4b32f7c3b854d9f5347b
f07a4",
 "LastObservedAt": "2019-08-06T05:22:54Z",
 "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
 "ProductFields": {
  "action/actionType": "NETWORK_CONNECTION",
  "action/networkConnectionAction/blocked": "false",
  "action/networkConnectionAction/connectionDirection": "INBOUND",
  "action/networkConnectionAction/localPortDetails/port": "22",
  "action/networkConnectionAction/localPortDetails/portName": "SSH",
  "action/networkConnectionAction/protocol": "TCP",
  "action/networkConnectionAction/remoteIpDetails/country/countryName": "China",
  "action/networkConnectionAction/remoteIpDetails/geoLocation/lat": "34.7725",
  "action/networkConnectionAction/remoteIpDetails/geoLocation/lon": "113.7266",
  "action/networkConnectionAction/remoteIpDetails/ipAddressV4": "10.10.10.72",
  "action/networkConnectionAction/remoteIpDetails/organization/asn": "56047",
  "action/networkConnectionAction/remoteIpDetails/organization/asnOrg": "China Mobile
communications corporation",
  "action/networkConnectionAction/remoteIpDetails/organization/isp": "China Mobile
Guangdong",
  "action/networkConnectionAction/remoteIpDetails/organization/org": "China Mobile",
  "action/networkConnectionAction/remotePortDetails/port": "33242",
  "action/networkConnectionAction/remotePortDetails/portName": "Unknown",
  "archived": "false",
  "aws/securityhub/CompanyName": "Amazon",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-
2::product/aws/guardduty/arn:aws:guardduty:us-west-
2:111111111111:detector/50b2ea07131dbe1530c23facb594b1fa/finding/8cb632a4b32f7c3b854d9f5347b
f07a4",
  "aws/securityhub/ProductName": "GuardDuty",
  "aws/securityhub/SeverityLabel": "MEDIUM",
  "count": "7",
  "detectorId": "50b2ea07131dbe1530c23facb594b1fa",
  "resourceRole": "TARGET"
 },
 "RecordState": "ACTIVE",
 "Resources": [
  {
  "Details": {
   "AwsEc2Instance": {
    "ImageId": "ami-f2c2408a",
     "IpV4Addresses": [
       "10.10.10.20",
       "10.0.0.137"
   ],
   "LaunchedAt": "2019-08-05T17:10:47.000Z",
   "SubnetId": "subnet-931605f1",
   "Type": "m5.4xlarge",
   "VpcId": "vpc-c66576a4"
  }
  },
  "Id": "arn:aws:ec2:us-west-2:111111111111:instance/i-0799ee6e490c078c5",
  "Partition": "aws",
  "Region": "us-west-2",
  "Tags": {
   "Name": "elasticsearch-node-coordinator"
  },
  "Type": "AwsEc2Instance"
  }
 ],
 "SchemaVersion": "2018-10-08",
 "Severity": {
 "Normalized": 40,
 "Product": 2
},
"Title": "310.10.10.72 is performing SSH brute force attacks against i-0799ee6e490c078c5. ",
"Types": [
 "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
],
 "UpdatedAt": "2019-08-06T05:28:24.425Z",
 "WorkflowState": "NEW",
 "phCustId": 1,
 "serverIp": "10.10.10.22",
 "serverName": "amzon.com"
}
```

Box.com

- Integration Points
- Box API Integration
- Configuration

Integration Points

Protocol	Information Discovered	Used For
Box.com API		Security and Compliance

Box API Integration

FortiSIEM can pull audit events from Box.com Cloud Service via Box API.

Configuration

- Configuring Box.com Service
- Configuring FortiSIEM

Configuring Box.com Service

Create an account to be used for FortiSIEM communication.

- A general account can pull user events
- An Admin account can pull enterprise events

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Box.com Box
Access Protocol	Box API
Account	Choose **Account** as the email address for

Settings	Description
	the account created while Configuring Box.com Service.
Organization	Choose the **Organization** if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

3. After clicking **Save**, you will be redirected to the Box.com website. Enter the credentials for Box.com and click **Authorize**.
4. Click **Grant Access to Box**. You should see that the authorization for FortiSIEM to access your Box.com account was successful.
5. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Set **IP/Host Name** to box.com.
   b. Select the Credential created in step 2a from the **Credentials** drop-down list.
   c. Click **Save**.
6. Select the entry from step 5, click the **Test** drop-down list and select **Test Connectivity** and make sure it succeeds, which implies that the credential is correct.
7. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Box.com Cloud Service using the Box.com API.
8. To see the received events, go to **ADMIN > Setup > Pull Events**, select the Box.com entry and click **Report**. The system will take you to the **ANALYTICS** tab and run a query to display the events received from Box.com in the last 15 minutes. You can modify the time interval to get more events.

Cisco Umbrella

FortiSIEM Support added: 6.3.2

Vendor: Cisco

Product Information: https://umbrella.cisco.com/

- What is Discovered and Monitored
- Configuration
- Sample Events

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Cisco Umbrella.

Protocol	Metrics Collected	Used For
AWS S3 Bucket API	DNS logs, Proxy logs, IP logs, Admin Audit logs	Security Monitoring

Configuration

- Setup in Cisco Umbrella
- Setup in FortiSIEM

Setup in Cisco Umbrella

Complete these steps from the Cisco Umbrella Portal.

1. Login to dashboard.umbrella.com.
2. Navigate to **Admin > Log Management**.
3. Navigate to Amazon S3.
4. Select the **Use Cisco-Managed S3 storage** radio button.
5. Select the closest geographically region to the FortiSIEM instance that will poll the logs.
6. Select the desired retention duration.
   Note: Since this will be ingested by FortiSIEM, it is recommended to select the shortest duration.
7. Click **Save**.
8. Click **Continue**.
9. On the final screen, record these values for Setup in FortiSIEM.
   - Data Path: This is the S3 bucket URL
   - Access Key
   - Secret Key
10. Click **Got It**.
11. Click **Continue**.
    Cisco Umbrella setup is now complete. However, it may take some time to activate.

Note: You can select company-managed s3 bucket, but you must provide an access key and secret with

appropriate permissions. Cisco managed takes away the difficulty with IAM permissions for S3 bucket access.

Setup in FortiSIEM

FortiSIEM processes events from Cisco Umbrella via the AWS S3 bucket API. Obtain your Access Key, Secret Key, and S3 bucket URL from the Cisco Umbrella Portal before proceeding.

Complete these steps in the FortiSIEM UI:

1. For Multi-tenant users, change the scope to the appropriate FortiSIEM organization.
2. Go to the **ADMIN > Setup > Credentials** tab.
3. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box, and click **Save** when done.

Settings	Description
Name	Enter a name for the credential.

Settings	Description
Device Type	Cisco Umbrella
Access Protocol	AWS_S3
Region	Enter the AWS region for the bucket that was created, which can be found by looking at the data path name. For example, `cisco-managed-us-west-1`, means "us-west-1", so you would input `us-west-1` in the Region field.
Bucket	Enter the Bucket value that appears before the forward slash, e.g. cisco-managed-us-west-1.
Prefix	This is the part with the forward slash. **Note**: Make sure to include a single forward slash at the end of the string only, e.g. 1234567_ b123456789f1e2a3a412345410123ffcd456789 e0**/** If the prefix is entered as any of the following ways */xxxx/* *xxxx* */xxxx* the integration will fail. The prefix must be entered as *xxxx/* **Correct Example**: 1234567_ b123456789f1e2a3a412345410123ffcd456789 e0**/** **Incorrect Examples**: */*1234567_ b123456789f1e2a3a412345410123ffcd456789 e0/ 1234567_ b123456789f1e2a3a412345410123ffcd456789 e0
Access Key ID	Enter/paste the access key you acquired during the Cisco Umbrella setup.

Settings	Description
Secret Key	Enter/paste the secret key you acquired during the Cisco Umbrella setup.
Log Keyword	Leave the default option, which is `Cisco_Umbrella_Log`.
Description	Description about the device

4. In **Step 2: Enter IP Range to Credential Associations**, if you have more than one FortiSIEM collector, select the collector that will do the polling from the drop-down list. **Note**: A drop-down list will not appear if you only have one collector.
5. Click **New**.
   a. Select the credential name you created (during step 3a) from the **Credentials** drop-down list. The **IP/Host Name** field should auto populate the URL (reports.api.umbrella.com).
   b. Click **Save**.
6. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection.
7. Wait for approximately 5 minutes.
8. Navigate to **ANALYTICS**, and confirm that events appear.

Sample Events

```
//CiscoUmbrella-DNS-A-Query-Success
1 146.112.59.20 reports.api.umbrella.com Cisco_Umbrella_Log 5381234_
b617173610f6e6a12340410126fdba516751f0/dnslogs/2021-08-25/2021-08-25-21-20-ade8.csv.gz :
"2021-08-25 21:19:36","LAB-MACHINE","LAB-
MACHINE","192.168.10.218","99.99.99.25","Allowed","1 (A)","NOERROR","static-
asm.secure.skypeassets.com.","Chat,Instant
Messaging,Software/Technology,Infrastructure,Internet Telephony,Application","Roaming
Computers","Roaming Computers",""

//CiscoUmbrella-DNS-A-Query-Blocked
1 146.112.59.20 reports.api.umbrella.com Cisco_Umbrella_Log 5381234_
b617173610f6e6a12340410126fdba516751f0/dnslogs/2021-08-26/2021-08-26-19-00-44ea.csv.gz :
"2021-08-26 19:03:13","LAB-MACHINE","LAB-
MACHINE","192.168.10.218","99.99.99.25","Blocked","1
(A)","NOERROR","www.facebook.com.","Social Networking,Application,Application
Block","Roaming Computers","Roaming Computers","Application,Application Block"
```

Fortinet FortiCASB

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
API				Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, and search for "FortiCASB" to see the event types associated with this device.

Rules

No specific rules are written for FortiCASB but generic end point rules apply.

Reports

No specific reports are written for FortiCASB but generic end point rules apply.

Configuration

Configure FortiCASB to send logs to FortiSIEM in the supported format (see Sample event below)

Setup in FortiCASB

Take the following steps in FortiCASB.

1. Login to FortiCASB with your account.
2. At the top right corner, click on the Switch Company icon.
3. Click **Manage Company** to access the company setting.
4. Select the **API Setting** tab.
5. Click **Generate New** to generate a new API credential.
6. EIn the Credential field, enter a credential name and click **Generate Credential**.
7. Copy the credential information to be used later to call the FortiCASB API.
   Note: The credential will only be shown once, so keep it in a private and secured place.
   The generated credential can be used repeatedly as long as it is not revoked on FortiCASB.

Setup in FortiSIEM

FortiSIEM processes events from this via the Fortinet FortiCASB API. Make sure to complete Setup in FortiCASB before proceeding here.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Fortinet FortiCASB
Access Protocol	FortiCASB_API
Pull Interval	5 minutes
Token	Provide the authorization token from your account.
Confirm Token	Provide the authorization token from your account to confirm.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Select the name of your credential from the **Credentials** drop-down list. The **IP/Host Name** field will auto populate with "www.forticasb.com".
   b. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiCASB.
5. To see the jobs associated with FortiCASB, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "FortiCASB" in the search box.

Sample Events

```
[FortiCASB-EVENT] = {
   "alertType":"Data Analysis",

"applicationId":"Y2lzY29zcGFyazovL3VzL09SR0FOSVpBVElPTi84NGI0NDZlMi0xYTU5LTQyZjQtOGVkMy05YmY
4MjdiN2ZlMjg",
   "buId":84,
   "companyId":"62598",
   "contextName":"DLP Birthdate Policy",
   "createTime":1621250006181,
   "defineType":"Predefined",
   "displayOperation":"Upload File",
   "eventId":"62598-Webex-58cb1d3b6f30326cfca5e64d2f96fa5d",
   "eventIdList":[
      "62598-Webex-58cb1d3b6f30326cfca5e64d2f96fa5d"
   ],

"fileId":"Y2lzY29zcGFyazovL3VybjpURUFNOnVzLXdlc3QtMl9yL0NPTlRFTlQvOWI2YjUzNzAtYjZmZi0xMWViLW
E0NjAtMDE0ZTAzYTk3NmI3LzA",
   "id":"d6e52513ee1069437704271f1144d981",
   "matches":1,
   "object":"01-ssn-usercollaborator.doc",

"objectId":"Y2lzY29zcGFyazovL3VybjpURUFNOnVzLXdlc3QtMl9yL0NPTlRFTlQvOWI2YjUzNzAtYjZmZi0xMWVi
LWE0NjAtMDE0ZTAzYTk3NmI3LzA",
   "objectType":"DOCUMENT",
   "phCustId":1,
   "policyCode":"FC-ACT-018",
   "policyId":"13285945",
   "policyName":"DLP Birthdate Policy",
   "resultDesc":"File \"  01-ssn-usercollaborator.doc  \"Matches the DLP Birthdate 1 times
(s), the matched content are: \n(1) *****1972 \n\n\n null\n ",
   "serverHostName":"www.forticasb.com",
   "serverIp":"34.212.75.194",
   "service":"Webex",
   "severity":"Alert",
   "timestampUUID":"d6e52513ee1069437704271f1144d981",
   "updateTime":1621250006000,
   "user":"testadmin1@forticasb.com",

"userId":"Y2lzY29zcGFyazovL3VzL1BFT1BMRS8zZGVmNDBhNC1kYTI1LTQ0ODctODFlOS0zNWJjYzk5MTA2YTA",
   "userName":"Test admin",
   "violationActivity":"WEBEX_CREATED_MESSAGES"
}
```

Google Cloud Platform (GCP)- Pub/Sub Integration

FortiSIEM Support added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Google

Product Information: https://cloud.google.com/

What is Discovered and Monitored

- Event Types
- Rules
- Reports
- Dashboard
- Configuration

What is Discovered and Monitored

Protocol	Logs Collected	Used For
Google Cloud Pub/Sub SDK	Admin Activity audit logs, Data Access Audit logs, System Event audit logs, Policy Denied audit logs. Arbitrary custom log ingestion via Pub/Sub topic.	GCP Audit Log ingestion, or Custom Log Ingestion

Event Types

In **ADMIN > Device Support > Event Types**, search for "GCP_A" in the **Search** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "GCP:" in the main content panel **Search...** field to see the rules associated with this application or device.

In 6.3.1 the following rules are available:

- GCP: Firewall Rule Created
- GCP: Firewall Rule Deleted
- GCP: Firewall Rule Patched
- GCP: IAM Custom Role Created
- GCP: IAM Custom Role Deleted
- GCP: IAM Member assigned role of type admin or owner
- GCP: Logging Sink Deleted, GCP: Logging Sink Updated
- GCP: Pub/Sub Subscription Created
- GCP: Pub/Sub Subscription Deleted
- GCP: Pub/Sub Topic Created
- GCP: Pub/Sub Topic Deleted
- GCP: Service Account Access Key Created
- GCP: Service Account Access Key Deleted
- GCP: Service Account Created
- GCP: Service Account Deleted
- GCP: Service Account Disabled
- GCP: Storage Bucket IAM Permissions Modified
- GCP: Storage Bucket Updated
- GCP: Storage or Logging Bucket Deleted
- GCP: VPC Network Deleted
- GCP: VPC Route Added
- GCP: VPC Route Deleted

Reports

There are many reports defined in **RESOURCES > Reports**. Search for "GCP:" in the main content panel **Search...** field.

In 6.3.1, the following reports are available:

- GCP: Firewall Rule Created, Deleted, or Changed
- GCP: IAM Custom Roles Created or Deleted
- GCP: IAM Policy Change Audit Report
- GCP: Logging Sinks Created, Updated, or Deleted
- GCP: Pub/Sub Subscriptions Created or Deleted
- GCP: Pub/Sub Topic Created or Deleted
- GCP: Service Account Access Keys Created or Deleted
- GCP: Service Accounts Created, Deleted, or Disabled
- GCP: Storage Bucket IAM Permissions Modified
- GCP: Storage Buckets Updated
- GCP: Storage or Logging Bucket Deleted
- GCP: Top Admin Activity Events by Principal
- GCP: Top Admin Activity Events by Source IP
- GCP: Top Data Access Events by Principal
- GCP: Top Data Access Events by Source IP
- GCP: Top Event Types by Count
- GCP: Top Traffic by Country
- GCP: VPC Network Created or Deleted
- GCP: VPC Routes Created or Deleted

Dashboard

A standard GCP Audit Dashboard can be found by navigating to **DASHBOARD**, and selecting **GCP Dashboard** from the Dashboard drop-down list.

Configuration

- Google Cloud Platform Pub/Sub Setup
- FortiSIEM Service Account Setup
- FortiSIEM Configuration
- Custom Log Integration

Google Cloud Platform Pub/Sub Setup

Google Cloud Platform (GCP) Log Flow: GCP audit logs sink -> Pub/Sub topic for FortiSIEM -> FortiSIEM ingest with standard log header appended

To set up GCP Pub/Sub:

1. Create a topic by taking the following steps:
    a. Go to Pub/Sub Service in GCP console.
    b. Select the project where the topic should reside.
    c. In the Create Topic dialog boxes, enter the following options:
        i. In the **Topic id** field, enter "fortisiem-topic", or a desired name for the topic.
        ii. For **Leave option**, make sure the checkbox next to "**Add a default subscription**" is checked.
        iii. When done, click **CREATE TOPIC**.
        iv. Notate the topic name. Example: projects/fortisiem-integration-1111/topics/fortisiem-topic
        v. Click on **Subscriptions** and notate the subscription name. Example: projects/fortisiem-integration-1111/subscriptions/fortisiem-topic-sub
2. Turn on audit logs for all services by taking the following steps:

    Note: Not all auditing is on by default, so this configuration is necessary.

    a. Go to **IAM & Admin**.
    b. Select **Audit Logs** on the left hand toolbar.
    c. Click the **Default Audit Config** button at the top of the screen.
    d. Select all desired log options.

        For the most verbose log information, make sure to select the following 4 boxes: **Admin Read**, **Admin Write**, **Data Read**, and **Data Write**.

        For minimal logging, only select **Admin Read** and **Admin Write**.

        Note: Optionally, VPC flows and Firewall Rule logs can be configured through the VPC network menu by taking the following steps:
        For Firewall rules, you must select each one you would like to enable with logs, edit, and then select the Logs radio button to turn on. Repeat for each desired Firewall rule.

        i. Go to **VPC networks**.
        ii. Select your desired Subnet.
        iii. Click the **Flow logs** drop-down list.
        iv. Set sampling interval to 5 seconds, and leave the rest as default.
    e. Click **Done**.
3. Create an aggregated sink with the topic in pub/sub as the destination. The destination topic can be created in any Cloud project in any organization if the service account from the log sink has permission to write to the destination.

    The serviceAccount entry is returned from the create sink command that shows which identity must be added to the particular Pub/Sub topic as a role Pub/Sub Publisher.

    This identity represents a Google Cloud service account that has been created for the log export. Until you grant this identity, publisher permissions to the destination topic and log entry exports from this sink will fail. For more information, see step 4 for granting access for a resource.

    Take the following steps:

    a. Select the Gcloud console (**>_**) button on top right hand of your browser.
    b. Enter the following comand:

        ```
        gcloud organizations list
        ```
    c. You may be prompted to authorize the command. If so, select **yes**.
    d. Notate the Organization ID. Example: 87732091111
    e. Format your sink destination as `pubsub.googleapis.com/<pubsubtopic>`
    f. Run the following command if your project is tied to, or part of an organization; This command creates an organization wide sink called **fortisiem_sink** for all projects and folders, and sends all logs to the Pub/Sub

topic specified.

```
gcloud logging sinks create fortisiem_sink \
pubsub.googleapis.com/projects/fortisiem-integration-1111/topics/fortisiem-topic
--include-children \
--organization=<organization_id>
```

If your project is not tied to, or has no organization, use the project id instead. It will create a sink of this project only, meaning only the logs from this project will go into the topic.

You can repeat this command for each sink you’d like to create per project. You can modify the sink name for each to ensure uniqueness.

```
gcloud logging sinks create fortisiem_sink \
pubsub.googleapis.com/projects/fortisiem-integration-1111/topics/fortisiem-topic
--include-children \
--project=<project_id>
```

g. !**IMPORTANT**! Copy the output, and notate the service account created. It is required to permit the service to write to the pub/sub topic. Must be Pub/Sub Publisher.

   Example:

   Created [https://logging.googleapis.com/v2/organizations/87732091111/sinks/fortisiem_sink].

   Grant **serviceAccount**:`o111110938575-661167@gcp-sa-logging.iam.gserviceaccount.com` the **Pub/Sub Publisher role** on the topic.

   More information about sinks can be found at https://cloud.google.com/logging/docs/export/configure_export

4. Configure aggregated sink service account for the given organization (from step 3) to publish to the created topic (created in step 1) by taking the following steps:
   a. Go to the **Pub/Sub topics** service page.
   b. Select the project where the topic was created.
   c. Click on the topic (fortisiem-topic, or the topic name entered) from step 1.
   d. Click **Show Info Panel** on the right hand toolbar to show the **Permissions** tab.
   e. Click the **Add Member** button.
   f. Paste the service account created with the aggregated sink that you created earlier here.
   g. Apply role of Pub/Sub Publisher.
   h. Click **Add**.
      Pub/Sub is now set up.

FortiSIEM Service Account Setup

A service account for FortiSIEM is required to ingest logs from the Pub/Sub topic. To create this account, take the following steps:

1. Go to the **Service accounts** page.
2. Click **Create Service Account**.
3. Select the project in the drop-down list where the Pub/Sub topic exists.
4. In the **Service Account Name** field, enter "fortisiem-pubsub", or a desired name for the service account.
5. Click **Create**.
6. Click **Continue**.
7. Select **Role Pub/Sub Subscriber**.

8. Click **Continue**.
9. Click **Done**.

Now, a service account key is needed. To create a service account key, take the following steps:

1. Select your new service account.
2. Click on the **Keys** tab.
3. Click the **Add key** drop-down list, and select **Create new key**.
4. Select **JSON** as the Key type, and click **Create**.

A file download will be created with service account data. This file is required for FortiSIEM configuration. Store a secure copy.

FortiSIEM Configuration

The following items are required for FortiSIEM integration.

- The subscription name created under the Pub/Sub topic: e.g. **projects/fortisiem-integration-1111/subscriptions/fortisiem-topic-sub**
    - Locate the subscription name by going to the topic you created, selecting subscriptions, and clicking on the subscription name.

      Note: The subscription name will need to be entered into the Subscription Path field configuration for FortiSIEM.
- The Service Account JSON Key file.

Make sure you have completed these instructions if you do not have these items.

- Google Cloud Platform Pub/Sub Setup
- FortiSIEM Service Account Setup

To configure FortiSIEM, take the following steps:

1. Login to the FortiSIEM GUI.

   Note: If this SIEM has multiple organizations, change the scope to the desired organization level for ingesting logs.
2. Navigate to **ADMIN > Setup > Credentials**.
3. In **Step 1: Enter Credentials**, click **New** to create a new credential.
    a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
    b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Google Google Cloud Platform
Access Protocol	GOOGLE_Pub_Sub
Pull Interval	5 minutes (leave at default)
Subscription Path	Enter the subscription name from Google Cloud Platform.

Settings	Description
	Example: `projects/fortisiem-integration-1111/subscriptions/fortisiem-topic-sub`
Service Account Key	Click **Upload** and upload the JSON Service Account Key.
Log Keyword	Leave the default value of “GCP_AUDIT_LOG”. Changing this will break the parser. This uniquely identifies that every log in this Pub/Sub topic is from Google Cloud Audit logging.
Description	(Optional) Description about the instance.

   c. Click **Save**.

4. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.

   Note: If your SIEM organization has multiple FortiSIEM collectors, be sure to select which collector will do the polling. A drop-down list will appear to the right of the **Test** button if you have multiple collectors. If you only have 1 collector, or in Super only environments, no collectors, no drop-down list will appear.

   a. Select the name of your credential from the **Credentials** drop-down list.
   b. The **IP/Host Name** field will auto populate with google.com. This is normal, do not change it.
   c. Click **Save**.
5. To start polling, select the new mapping, click the **Test** drop-down list, and select **Test Connectivity without Ping**. It will take approximately 5 minutes for the initial poll job to kick off.
6. Once 5 minutes have passed, click **ANALYTICS**.
7. Click the **Edit Filters and Time Range...** field to run a query to see any Google Audit Logs.
   a. Select **Event Attribute**.
   b. Under **Attribute**, enter/select **Event Type**.
   c. Under **Operator**, select **CONTAIN**.
   d. Under **Value**, enter **GCP_AUDIT**.
   e. Click **Apply & Run** to execute.

Custom Log Integration

This integration is only needed if you are publishing custom logs to a Google Pub/Sub topic, and would like FortiSIEM to ingest those logs. Note that once the logs are ingested, you will still need to create a FortiSIEM parser for the log to be parsed and analyzed once ingested.

Log Flow: Custom logs from customer applications and systems -> Pub/Sub custom topic -> FortiSIEM ingest with custom log header appended

To integrate custom logs, take the following steps:

Note: In this process, the setup for a Pub/Sub topic is the same as normal integration, but instead of sinking GCP logs to the topic, you instead ingest your custom logs to the topic on your own.

1. Create a Pub/Sub topic.
2. Publish your custom logs to your topic. Your team will create a service account for your custom applications to send logs to this topic.
3. Create a service account with subscriber permissions to the topic for FortiSIEM. See FortiSIEM Service Account Setup.
4. Configure FortiSIEM with service account credential and subscription name, and enter the custom log header format. This step follows the exact instructions in FortiSIEM Configuration except for the need to change **Log Keyword** in the **Access Method Definition** dialog box. See Log Keyword Information for more information.

Log Keyword Information

Log Keyword is a critical component for the parsing of logs. If you are ingesting custom logs, FortiSIEM will prepend the string to the log. This is supposed to be a unique identifier to know what the custom logs are for parsing.

Example:

We publish the log file `{“attackName”:”REvil Compromise”,”hostname”:”host1”}` into a Pub/Sub topic. This is a log from Custom Application A for our example.

When we set up the FortiSIEM integration, we’ll do something to specify a log keyword to uniquely identify what type of logs these are.

When FortiSIEM ingests the log, it will appear in this format:

```
1 192.168.1.20 google.com CUSTOM_APP_A {“attackName”:”REvil
Compromise”,”hostname”:”host1”}
```

This is important for log parsing, as we can write a parser that matches this log header, to process these logs. Any log in this Pub/Sub topic gets this header. This helps us write parsing in a simplified manner, as not all logs are cleanly structured and helps identify what or where the logs are from originally.

For custom log parsing, see the NSE training documentation on the topic, or consult FortiCare Professional Services.

Google Workspace (Formerly G Suite and Google Apps)

FortiSIEM Support added: 4.8.1 (as Google Apps Audit)

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Google

Product: Workspace (Formerly G Suite / Google Apps)

Product Information: https://workspace.google.com/

Note: Older rules and reports use "Google Apps" to reference "Google Workspace".

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Dashboard
- Activity Auditing Collected Services
- Configuration
- Sample Events for Google Workspace Audit

What is Discovered and Monitored

Protocol	Logs Collected	Used For
Google Apps Admin SDK	Configuration Change, Account Create/Delete/Modify, Account Group Create/Delete/Modify, Document Create/Delete/Modify/Download, Document Permission Change, Logon Success, Logon Failure, Device compromise	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Google_Apps" and "Google Workspace" in the **Search** field to see the event types associated with this device.

Rules

There are many rules defined in **RESOURCES > Rules**. Search for "Google Workspace" in the main content panel **Search...** field.

Reports

There are many reports defined in **RESOURCES > Reports > Device > Application > Document Mgmt**. Search for "Google Apps" and "Google Workspace" in the main content panel **Search...** field.

Dashboard

A standard Google Apps Dashboard can be found by navigating to **DASHBOARD**, and selecting **Google Apps Dashboard** from the Dashboard drop-down list.

Activity Auditing Collected Services

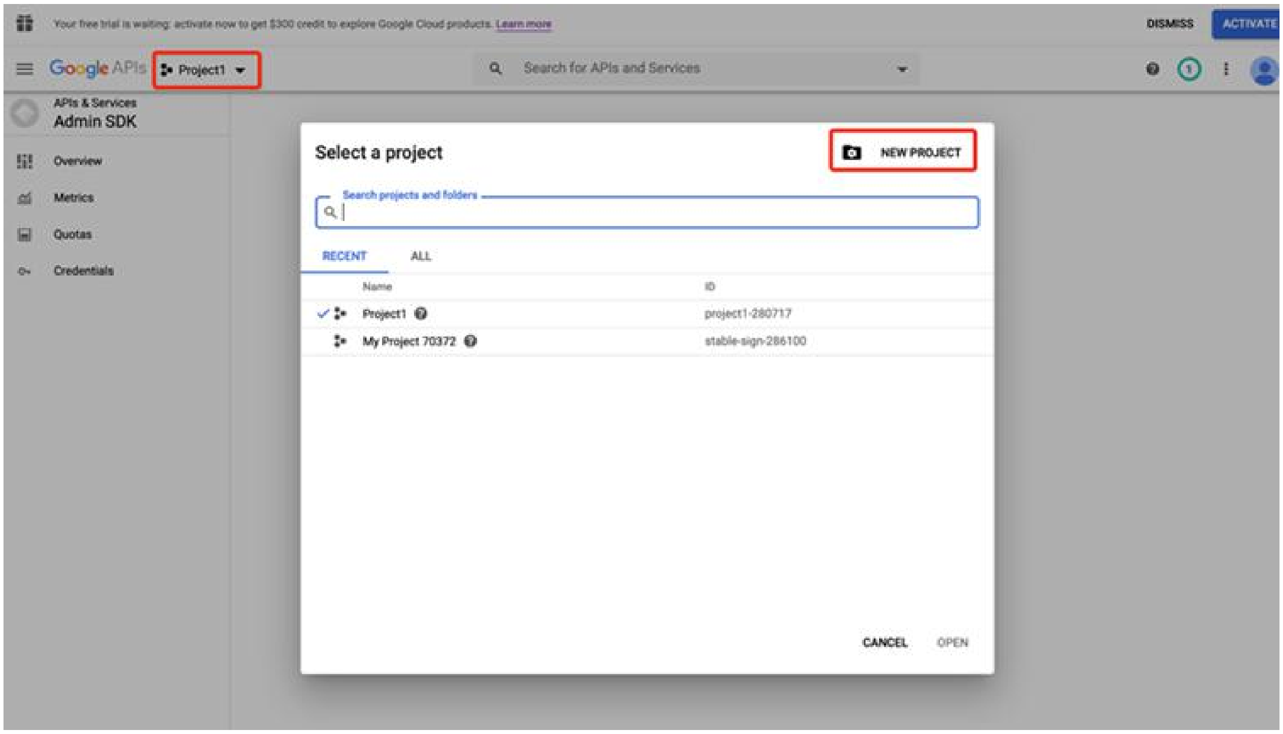
The following services have Activity Auditing collected: Access Transparency, Admin, Chrome, Context-Aware Access, Currents, Data Studio, Enterprise Groups, Google Calendar, Google Chat, Google Cloud Platform, Google Drive, Google Groups, Google Keep, Google Meet, Jamboard, Login, Mobile, OAuth Token, Rules, SAML, and User Accounts.

Configuration

- Create a Google Workspace Credential in Google API Console
- Define Google Workspace Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity

Create a Google Workspace Credential in Google API Console

1. Logon to Google API Console (https://console.developers.google.com).
2. Open the **Select a project** window and click **NEW PROJECT**.



Your free trial is waiting: activate now to get $300 credit to explore Google Cloud products. Learn more

Select a project

	Name	ID
✓	Project1	project1-280717
	My Project 70372	stable-sign-286100

3. Under the **New Project** window:
   a. **Project Name** - enter a name.
   b. Click **Create**.
4. Open the **Select a project** window and select the new project that you created in Step 2.
5. Under **Dashboard**, click **Enable API And Services** to find the **Admin SDK**.
6. Select **Admin SDK** and click **Enable** to activate the **Admin SDK** for this project.
7. Create a Service Account for this project:
   a. Under **Credentials**, click **Create Credentials > Service Account**.
   b. Enter the server account name.
   c. Click **Create**.
   d. Choose **Role** as **Project > Viewer**.
   e. Click **Continue>Done**.
8. Create key for the Service Account:
   a. Go to **Navigation Menu> IAM &Admin>Service Accounts**.
   b. Go to the **Service Account** table, choose the service account you create in Step 7.
   c. Click **Actions > Create Key**.
   d. Choose **Key type** as **JSON**.
   e. Click **Create**.
   f. A JSON file containing the Service Account credentials will be stored in your computer.

9. Enable Google Workspace Domain-wide delegation:
    a. Go to **Navigation Menu> IAM &Admin>Service Accounts**.
    b. Go to the **Service Account** table and choose the service account you created in Step 7.
    c. Click **Actions > Edit > SHOW DOMAIN-WIDE DELEGATION**.
    d. Check **Enable G Suite Domain-wide Delegation**.
    e. Enter **FortiSIEM** in the **Product name for the consent screen**.
    f. Click **Save**.
10. View Client ID:
    a. Go to **Navigation Menu> IAM &Admin>Service Accounts**.
    b. Go to the **Service Account** table and choose the service account you created in Step 7.
    c. Click **Actions > Edit > SHOW DOMAIN-WIDE DELEGATION**.
    d. You can find a **Client ID**.
11. Delegate **domain-wide authority** to the service account created in Step 7.
    a. Go to your Google Workspace domain's Admin console (https://admin.google.com).
    b. Select **Security** from the list of controls. If you don't see **Security** listed, select **More controls** from the gray bar at the bottom of the page, then select **Security** from the list of controls.
    c. Select **Advanced settings** from the list of options.
    d. Click **Manage domain wide delegation** in the **Domain wide delegation** section.
    e. Click **Add new**.
    f. In the **Client ID** field, enter the service account's Client ID you obtained in Step 10d.
    g. In the **OAuth scopes(comma-delimited)** field, enter the following scope that FortiSEM should be granted access to:
    https://www.googleapis.com/auth/admin.reports.audit.readonly
    h. Click **Authorize**.

Define Google Workspace Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential:
    a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Google Google Apps
Access Protocol	Google Apps Admin SDK
Account Name	Enter the **User Name** (this is the account name to log in to the Admin console)
Service Account Key	Upload the JSON credential file (see Step 8f in Create a Google Workspace Credential in Google API Console).

Settings	Description
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter "google.com" in the **IP/Host Name** field.
   b. Select the name of the credential created in Define Google Workspace Credential in FortiSIEM from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Google Audit Log Collection.

Sample Events for Google Workspace Audit

- Logon Success
- Logon Failure
- Create User
- Delete User
- Move User Settings

Logon Success

```
<134>Jan 21 19:29:21 google.com java: [Google_Apps_login_login_success]:[eventSeverity]=PHL_
INFO,[actor.profileId]=117858279951236905887,[id.time]=2016-09-09T06:53:58.000Z,
[id.applicationName]=login,[kind]=admin#reports#activity,[id.customerId]=C01lzy8ye,
[id.uniqueQualifier]=883030195151552102З,[event.parameters.login_type]=google_password,
[event.type]=login,[ipAddress]=45.79.100.103,[actor.email]=api1@accelops.net,
[event.name]=login_success,[etag]=""6KGrH_
UY2JDZNpgjPKUOF8yJF1A/Nfrg2SFjlC2gR6pJtpP2scVidmc""",Google_Apps_login_login_success,login_
success,1,45.79.100.103,
```

Logon Failure

```
<134>Jan 21 19:29:21 google.com java: [Google_Apps_login_login_failure]:
[eventSeverity]=PHL_INFO,[actor.profileId]=117858279951236905887,
[id.applicationName]=login,[kind]=admin#reports#activity,[event.parameters.login_
type]=google_password,[ipAddress]=45.79.100.103,[event.name]=login_failure,[id.time]=2016-
09-19T09:27:51.000Z,[id.customerId]=C01lzy8ye,[id.uniqueQualifier]=4795688196368428241,
[event.type]=login,[actor.email]=api1@accelops.net,[etag]=""6KGrH_
UY2JDZNpgjPKUOF8yJF1A/v5zsUPNoEdXLLK79zQpBcuxNbQU"",[event.parameters.login_failure_
type]=login_failure_invalid_password",Google_Apps_login_login_failure,login_
failure,1,45.79.100.103,
```

Create User

```
<134>Jan 21 19:29:20 google.com java: [Google_Apps_USER_SETTINGS_CREATE_USER]:
[eventSeverity]=PHL_INFO,[actor.callerType]=USER,[actor.profileId]=117858279951236905887,
[id.applicationName]=admin,[kind]=admin#reports#activity,[ipAddress]=45.79.100.103,
[event.name]=CREATE_USER,[id.time]=2016-09-19T09:22:44.646Z,[id.customerId]=C01lzy8ye,
[id.uniqueQualifier]=-8133102622954793216,[event.type]=USER_SETTINGS,
[event.parameters.USER_EMAIL]=test-user@accelops.org,[actor.email]=api1@accelops.net,
[etag]=""6KGrH_UY2JDZNpgjPKUOF8yJF1A/R5GJyWG9YHSiGRvo3-8ZBM0ZlL0""",Google_Apps_USER_
SETTINGS_CREATE_USER,CREATE_USER,1,45.79.100.103,
```

Delete User

```
 <134>Jan 21 19:29:20 google.com java: [Google_Apps_USER_SETTINGS_DELETE_USER]:
[eventSeverity]=PHL_INFO,[actor.callerType]=USER,[actor.profileId]=117858279951236905887,
[id.applicationName]=admin,[kind]=admin#reports#activity,[ipAddress]=45.79.100.103,
[event.name]=DELETE_USER,[id.time]=2016-09-19T09:22:28.582Z,[id.customerId]=C01lzy8ye,
[id.uniqueQualifier]=-4630441819990099585,[event.type]=USER_SETTINGS,[event.parameters.USER_
EMAIL]=test-user@accelops.org,[actor.email]=api1@accelops.net,[etag]=""6KGrH_
UY2JDZNpgjPKUOF8yJF1A/08MaodxPU6Zv7s6vJtuUQW9ugx0""",Google_Apps_USER_SETTINGS_DELETE_
USER,DELETE_USER,1,45.79.100.103,
```

Move User Settings

```
<134>Jan 21 19:29:20 google.com java: [Google_Apps_USER_SETTINGS_MOVE_USER_TO_ORG_UNIT]:
[eventSeverity]=PHL_INFO,[actor.callerType]=USER,[actor.profileId]=117858279951236905887,
[event.parameters.ORG_UNIT_NAME]=/test,[id.applicationName]=admin,
[kind]=admin#reports#activity,[ipAddress]=45.79.100.103,[event.name]=MOVE_USER_TO_ORG_UNIT,
[id.time]=2016-09-19T09:24:25.285Z,[id.customerId]=C01lzy8ye,[id.uniqueQualifier]=-
6704816947489240452,[event.type]=USER_SETTINGS,[event.parameters.USER_EMAIL]=test-
user@accelops.org,[actor.email]=api1@accelops.net,[event.parameters.NEW_VALUE]=/,
[etag]=""6KGrH_UY2JDZNpgjPKUOF8yJF1A/r1v9DiPZbL06fXFFjJlrWf2s3qI""",Google_Apps_USER_
SETTINGS_MOVE_USER_TO_ORG_UNIT,MOVE_USER_TO_ORG_UNIT,1,45.79.100.103,,
```

Microsoft Azure Audit

- What is Discovered and Monitored
- Event Types
- Configuration
- Sample Events for Microsoft Azure Audit

What is Discovered and Monitored

Protocol	Information Discovered	Information Collected	Used For
Azure CLI	None	Audit Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Azure Audit" in the **Search** field to see the event types associated with this device.

Configuration

You must define a user account in Azure for use by FortiSIEM to pull Audit logs. Use any of the following roles:

- Owner
- Reader
- Monitoring Reader
- Monitoring Contributor
- Contributor

FortiSIEM recommends using the 'Monitoring Reader' role, which is the least privileged to do the job.

Take the following steps for configuration.

- Create Microsoft Azure Audit Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity in FortiSIEM

Create Microsoft Azure Audit Credential in FortiSIEM

Complete these steps in the FortiSIEM UI after logging into the FortiSIEM supervisor node:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Azure Audit
Access Protocol	Azure CLI
Password Config	Choose Manual, CyberArk, or RAX_MSCloud from the drop down list. For Manual credential method, enter the username and credentials for an Azure account. FortiSIEM recommends using 'Monitoring Reader' role for this account. For CyberArk or RAX_MSCloud, see Password Configuration.
Azure Subscription ID	Enter the 32-digit GUID associated with your Azure subscription. In 6.3.0, to enter multiple subscription IDs, separate each ID by a space. Examples: Entering one subscription ID: a0123bcd-e456-6f78-9112-gh3i4j56k789 Entering two subscription IDs: a0123bcd-e456-6f78-9112-gh3i4j56k789 z9876yxv-u543-2t10-9876-sr5q4p32o109
Account Env	In 6.3.0, you can choose **AzureCloud**, **AzureChinaCloud**, **AzureGermanCloud**, or **AzureUSGovernmentCloud**. Selecting **AzureUSGovernmentCloud** applies a GCC High environment. **Note**: Prior to 6.3.0, the Azure CLI Agent only supported Global Azure, and did not support Azure China Cloud, Azure German Cloud, nor Azure US Government Cloud.
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity in FortiSIEM

When logged in to the FortiSIEM Supervisor node, take the following steps.

1. Go to **ADMIN > Setup > Credentials**.
2. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
    a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
    b. Select the name of the credential created in the "Microsoft Azure Audit Credential" step from the **Credentials** drop-down list.
    c. Click **Save**.
3. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection.
4. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Microsoft Audit Log Collection.

Sample Events for Microsoft Azure Audit

```
2016-02-26 15:19:10 FortiSIEM-Azure,
[action]=Microsoft.ClassicCompute/virtualmachines/shutdown/action,
[caller]=Cuiping.Wang@shashiaccelops.onmicrosoft.com,[level]=Error,
[resourceId]=/subscriptions/3ed4ee1c-1a83-4e02-a928-
7ff5e0008e8a/resourcegroups/china/providers/Microsoft.ClassicCompute/virtualmachines/china,
[resourceGroupName]=china,[eventTimestamp]=2016-02-14T06:12:18.5539709Z,[status]=Failed,
[subStatus]=Conflict,[resourceType]=Microsoft.ClassicCompute/virtualmachines,
[category]=Administrative
```

Microsoft Office 365 Audit

FortiSIEM Support added: 4.8.1

FortiSIEM last modification: 6.3.0

Vendor version tested: Not Provided

Vendor: Microsoft

Product Information: https://www.microsoft.com/en-us/microsoft-365/business

What is Discovered and Monitored

Office 365 Activity Type	Operation
File and folder activities	FileAccessed, FileCheckedIn, FileCheckedOut, FileCopied, FileDeleted,FileCheckOutDiscarded, FileDownloaded, FileModified, FileMoved, FileRenamed, FileRestored, FileUploaded
Sharing and access request activities	AccessRequestAccepted, SharingInvitationAccepted, CompanyLinkCreated, AccessRequestCreated, AnonymousLinkCreated, SharingInvitationCreated, AccessRequestDenied, CompanyLinkRemoved, AnonymousLinkRemoved, SharingSet, AnonymousLinkUpdated, AnonymousLinkUsed, SharingRevoked, CompanyLinkUsed, SharingInvitationRevoked
Synchronization activities	ManagedSyncClientAllowed, UnmanagedSyncClientBlocked, FileSyncDownloadedFull, FileSyncDownloadedPartial, FileSyncUploadedFull, FileSyncUploadedPartial
Site administration activities	ExemptUserAgentSet, SiteCollectionAdminAdded, AddedToGroup, AllowGroupCreationSet, CustomizeExemptUsers, SharingPolicyChanged, GroupAdded, SendToConnectionAdded, SiteCollectionCreated, GroupRemoved, SendToConnectionRemoved, PreviewModeEnabledSet, LegacyWorkflowEnabledSet, OfficeOnDemandSet, NewsFeedEnabledSet, PeopleResultsScopeSet, SitePermissionsModified, RemovedFromGroup, SiteRenamed, SiteAdminChangeRequest, HostSiteSet, GroupUpdated
Exchange mailbox activities	Copy, Create, SoftDelete, Move, MoveToDeletedItems, HardDelete, SendAs, SendOnBehalf, Update, MailboxLogin

Office 365 Activity Type	Operation
Sway activities	SwayChangeShareLevel, SwayCreate, SwayDelete, SwayDisableDuplication, SwayDuplicate, SwayEdit, EnableDuplication, SwayRevokeShare, SwayShare, SwayExternalSharingOff, SwayExternalSharingOn, SwayServiceOff, SwayServiceOn, SwayView
User administration activities	Add user, Change user license, Change user password, Delete user, Reset user password, Set force change user password, Set license properties, Update user
Group administration activities	Add group, Add member to group, Delete group, Remove member from group, Update group
Application administration activities	Add delegation entry, Add service principal, Add service principal credentials, Remove delegation entry, Remove service principal, Remove service principal credentials, Set delegation entry
Role administration activities	Add role member to role, Remove role member from role, Set company contact information
Directory administration activities	Add domain to company, Add partner to company, Remove domain from company, Remove partner from company, Set company information, Set domain authentication, Set federation settings on domain, Set password policy, Set DirSyncEnabled flag on company, Update domain, Verify domain, Verify email verified domain

Event Types

In **ADMIN > Device Support > Event Types**, search for "MS_Office365" in the **Search** field to see the event types associated with Office 365.

Reports

There are many reports defined in **RESOURCES > Reports > Device > Application > Document Mgmt**. Search for "Office365" in the main content panel **Search...** field.

Configuration in Office 365 Audit

- Enable Office 365 Audit Log Search
- Create the Office 365 API Credential

Enable Office 365 Audit Log Search

To be able to search audit logs, you must first enable Office 365 audit log search. For instructions on how to enable audit log search, see https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off.

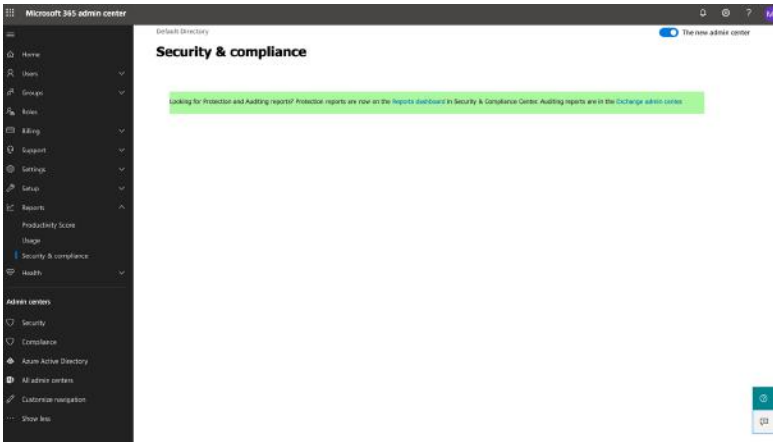
To use the Office 365 Management Activity API to access auditing data for your organization, you must enable audit log search in the Security & Compliance Center.

If you do not enable audit log search, you cannot access auditing data for your organization.

Before you can enable or disable audit log search for your Microsoft 365 organization, you must be assigned the Audit Logs role in the Exchange admin center.

Follow these steps to assign the Audit Logs role and enable audit log search for your organization.

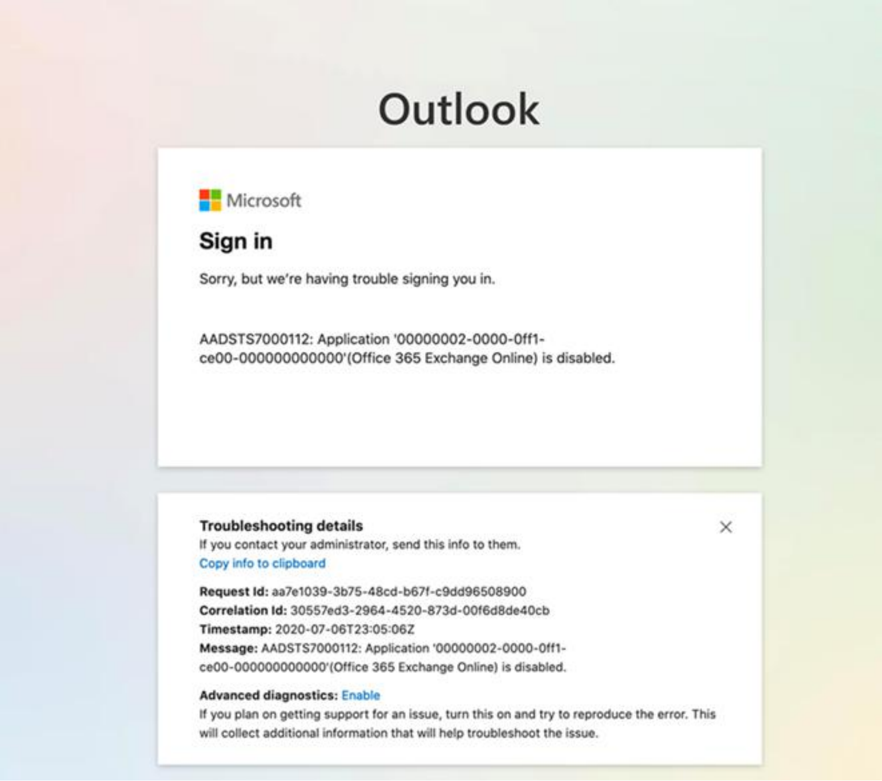
1. Log in to Microsoft Office Online: https://login.microsoftonline.com.
2. Click **Admin > Security & compliance**.



Security & compliance

Looking for Protection and Auditing reports? Protection reports are now on the Reports dashboard in Security & Compliance Center. Auditing reports are in the Exchange admin center.

3. Click **Exchange admin center**.
   If you receive the following alert, you must enable Office 365 Exchange Online before proceeding. In this case, go to Step 4. Otherwise, go to Step 6.



Sign in

Sorry, but we're having trouble signing you in.

AADSTS7000112: Application '00000002-0000-0ff1-ce00-000000000000'(Office 365 Exchange Online) is disabled.

Troubleshooting details

If you contact your administrator, send this info to them.

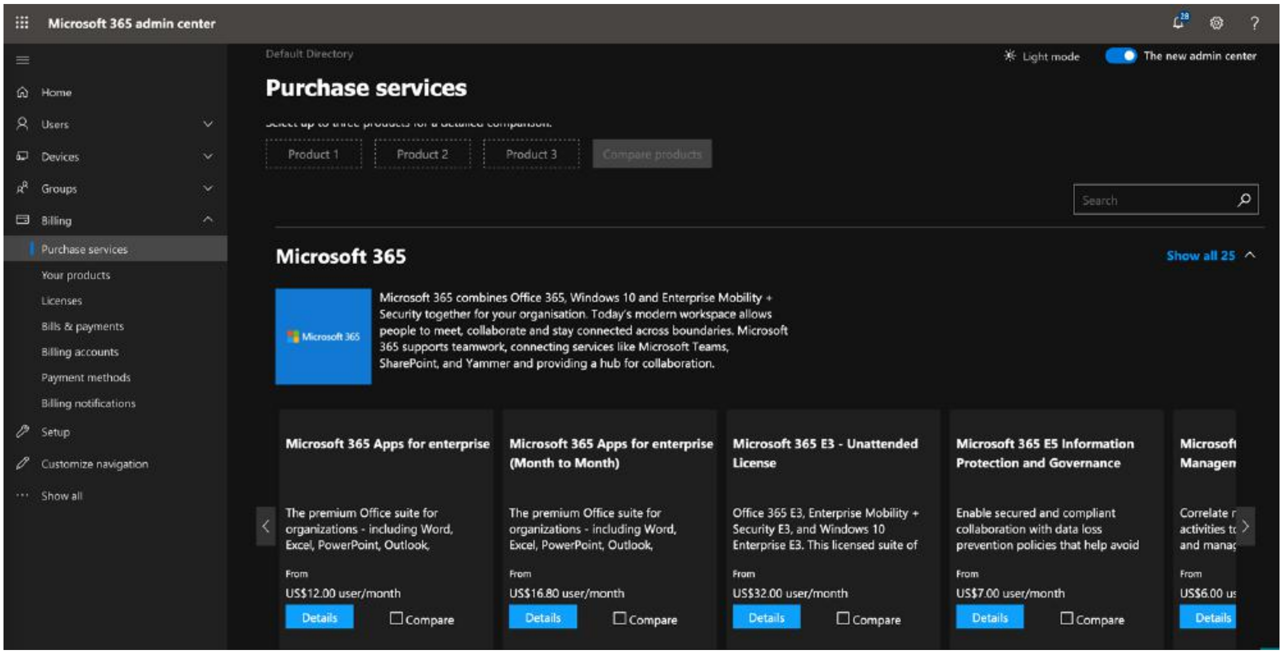
Copy info to clipboard

Request Id: aa7e1039-3b75-48cd-b67f-c9dd96508900
Correlation Id: 30557ed3-2964-4520-873d-00f6d8de40cb
Timestamp: 2020-07-06T23:05:06Z
Message: AADSTS7000112: Application '00000002-0000-0ff1-ce00-000000000000'(Office 365 Exchange Online) is disabled.

Advanced diagnostics: Enable

If you plan on getting support for an issue, turn this on and try to reproduce the error. This will collect additional information that will help troubleshoot the issue.

4. Click **Admin > Purchase services**.



Purchase services

Select up to three products for a detailed comparison.

Microsoft 365

Microsoft 365 combines Office 365, Windows 10 and Enterprise Mobility + Security together for your organisation. Today's modern workspace allows people to meet, collaborate and stay connected across boundaries. Microsoft 365 supports teamwork, connecting services like Microsoft Teams, SharePoint, and Yammer and providing a hub for collaboration.

Microsoft 365 Apps for enterprise

The premium Office suite for organizations - including Word, Excel, PowerPoint, Outlook,

From US$12.00 user/month

Microsoft 365 Apps for enterprise (Month to Month)

The premium Office suite for organizations - including Word, Excel, PowerPoint, Outlook,

From US$16.80 user/month

Microsoft 365 E3 - Unattended License

Office 365 E3, Enterprise Mobility + Security E3, and Windows 10 Enterprise E3. This licensed suite of

From US$32.00 user/month

Microsoft 365 E5 Information Protection and Governance

Enable secured and compliant collaboration with data loss prevention policies that help avoid

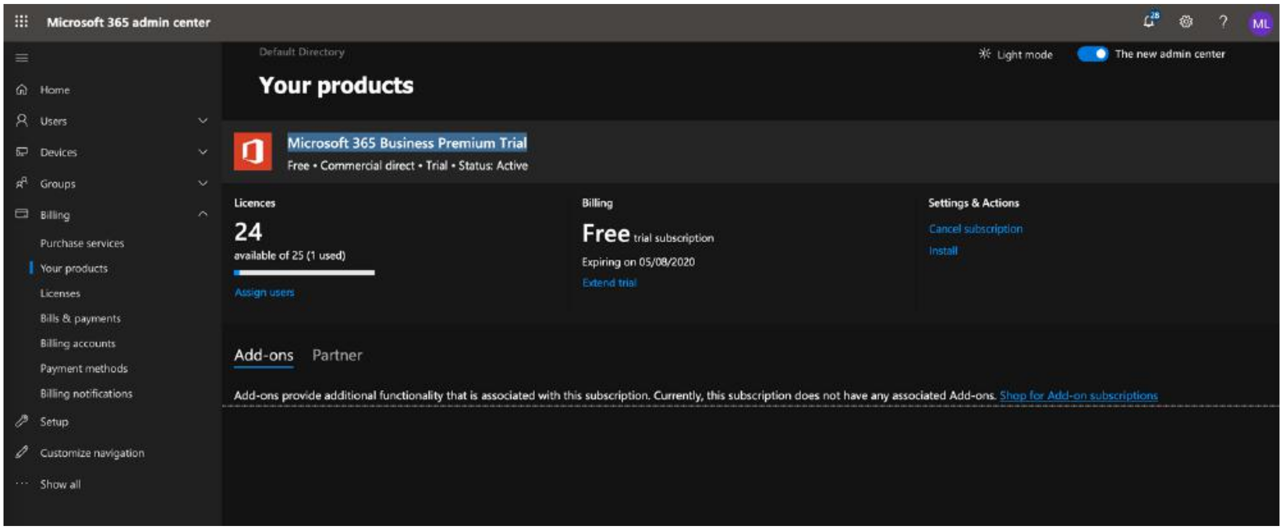
From US$7.00 user/month

Microsoft Managen

Correlate r activities tc and manag

From US$6.00 us

5. Select one of Microsoft 365 services. In this example, Microsoft 365 Business Premium Trial is selected.



Your products

Microsoft 365 Business Premium Trial

Free • Commercial direct • Trial • Status: Active

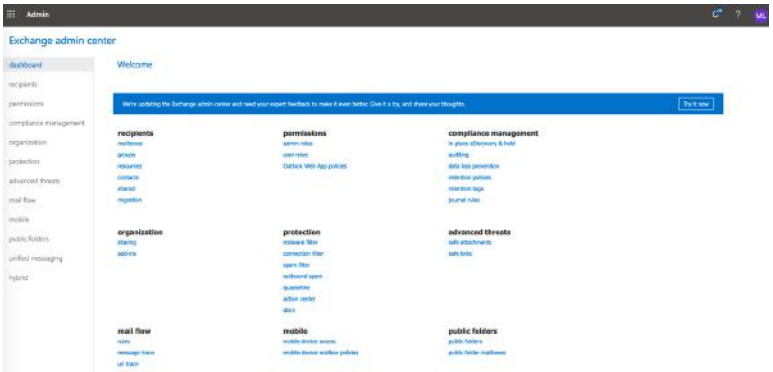
Licences: 24 available of 25 (1 used) — Assign users

Billing: Free trial subscription — Expiring on 05/08/2020 — Extend trial

Settings & Actions: Cancel subscription — Install

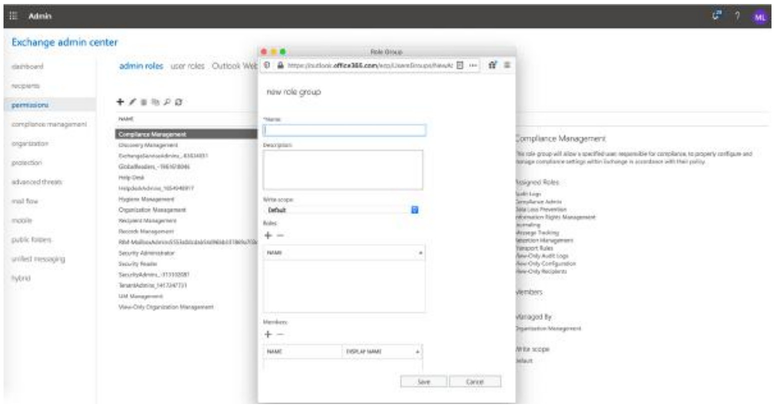
Add-ons provide additional functionality that is associated with this subscription. Currently, this subscription does not have any associated Add-ons. Shop for Add-on subscriptions

6. Click **Admin > Security & compliance > Exchange admin center**.



We're updating the Exchange admin center and need your expert feedback to make it even better. Give it a try, and share your thoughts.

7. Click **Exchange admin center > permissions > admin roles > New** to create a new role.



Compliance Management
Discovery Management
ExchangeServiceAdmins_-83634031
GlobalReaders_-1961678046
Help Desk
HelpdeskAdmins_1654946917
Hygiene Management
Organization Management
Recipient Management
Records Management
RIM-MailboxAdmins
Security Administrator
Security Reader
SecurityAdmins_-313100081
TenantAdmins_1417247731
UM Management
View-Only Organization Management

Compliance Management

This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.

Assigned Roles

Audit Logs
Compliance Admin
Data Loss Prevention
Information Rights Management
Journaling
Message Tracking
Retention Management
Transport Rules
View-Only Audit Logs
View-Only Configuration
View-Only Recipients

Members

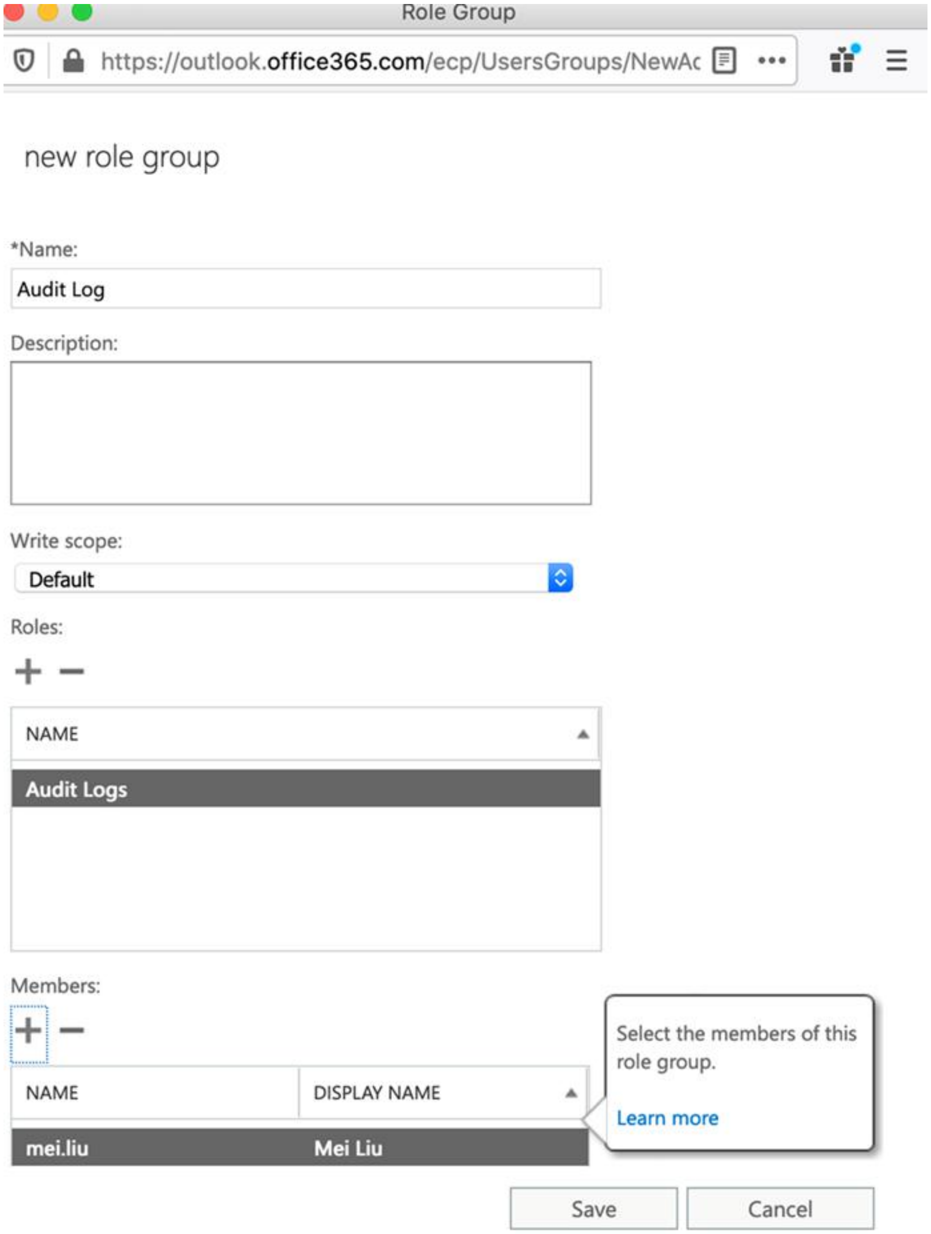
Managed By

Organization Management

Write scope

Default

8. Select **Audit Logs Roles** and add the members you want to add the group. Click **Save**.



new role group

*Name:

Audit Log

Description:

Write scope:

Default

Roles:

NAME
Audit Logs

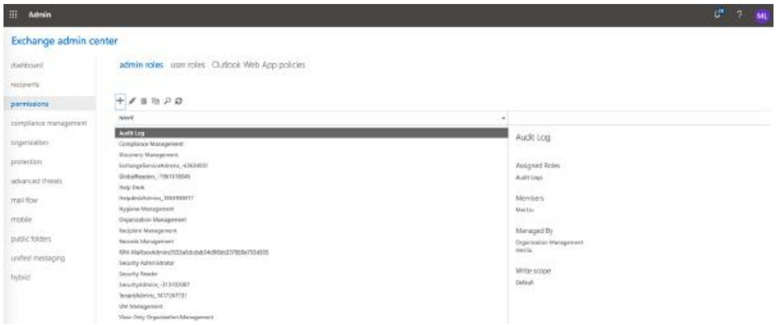
Members:

NAME	DISPLAY NAME
mei.liu	Mei Liu

Select the members of this role group.

Learn more

9. The **Audit Log** role will display in the **Exchange admin center > permissions > admin roles** table.



NAME
Audit Log
Compliance Management
Discovery Management
ExchangeServiceAdmins_-43634031
GlobalReaders_-1961518049
Help Desk
HelpdeskAdmins_1084988917
Hygiene Management
Organization Management
Recipient Management
Records Management
RIM-MailboxAdmins5553a0dcdab54d86bcd37868e7934385
Security Administrator
Security Reader
SecurityAdmins_-313102087
TenantAdmins_1437247731
UM Management
View-Only Organization Management

Audit Log

Assigned Roles

Audit Logs

Members

Mei Liu

Managed By

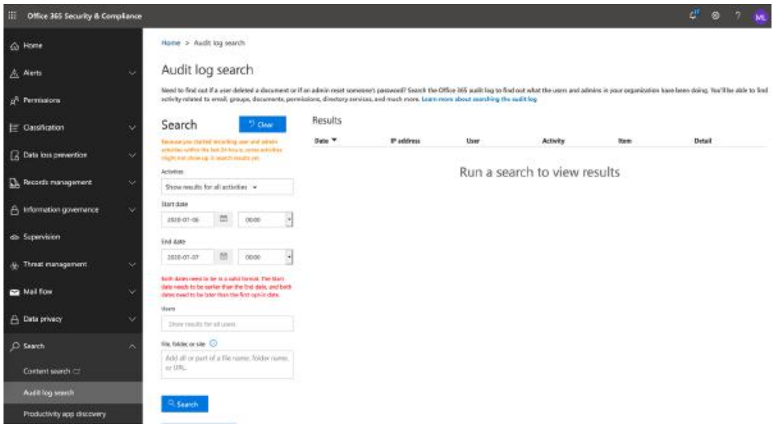
Organization Management

mei.liu

Write scope

Default

10. Go back to the Microsoft 365 Admin center.
11. Click **Security & compliance > Report dashboard**.
    When you first go into this page, it will ask you to enable Audit log. After you enable it, the page will display the **Search** button.



Create the Office 365 API Credential

Follow these steps to create the Office 365 API credential.

1. Login to https://portal.azure.com.
2. Click **All Services**.
3. Click **Azure Active Directory**.
4. Click **App Registrations** (on the right panel).
5. Click **New registration** and enter the following information:
   Name: FSM

   Supported Account Types: Select **Accounts in any organizational directory (Any Azure AD directory – Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)**.

   Redirect URI: https://your.internal.fsm.ip
6. Click **Register**:
   Copy the Application (client) ID to a text editor, you'll need this when entering Office 365 Credentials in FortiSIEM.

   Copy the Directory (tenant) ID to a text editor, you'll need this when entering Office 365 Credentials in FortiSIEM.
7. Click **Certificates & secrets** (on the right panel).
8. New client secret:
   Description: FSM

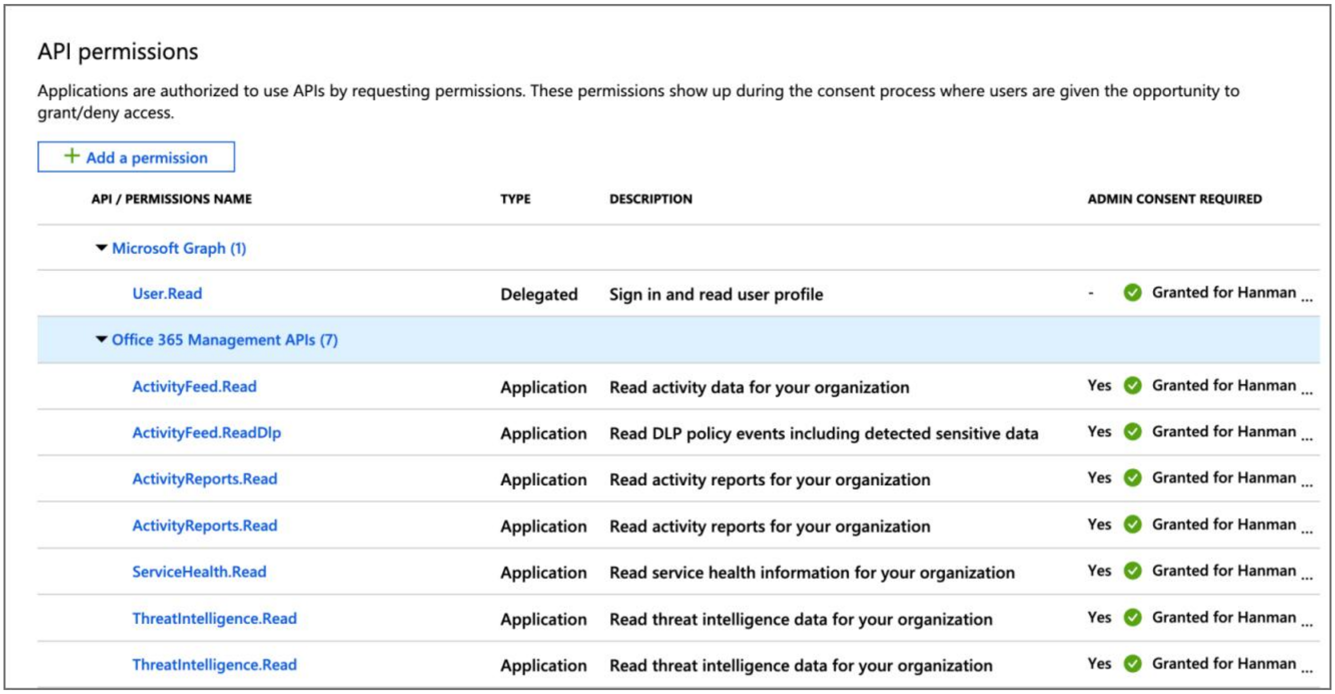
   Expires in: 2 years

   Copy the value (for example: `AC83J.6_nobD:G1Q=DJe/hFiB3BP4+a`) to a text editor. You will need this value when entering Office 365 Credentials in FortiSIEM.
9. Go to **API permissions** (left panel).
10. Click **Add a permission**.
11. Select **Office 365 Management APIs**.
12. Click **Application permissions** and expand all.
13. Select all permissions with "Read" access (we don't want to write). Click **Add permissions**.
    You will see a warning: "Permissions have changed." Users and/or admins will have to consent even if they have already done so previously.

    We'll need to approve all these permission grants.

14. Click **grant admin consent** and select **Yes** when you see the **Do you want to grant consent for the requested permissions for all accounts in your_organization?** alert. This will update any existing admin consent records this application already has to match what is listed below.

Sample API Permission



API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	
▾ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for Hanman ...
▾ Office 365 Management APIs (7)				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	✓ Granted for Hanman ...
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Yes	✓ Granted for Hanman ...
ActivityReports.Read	Application	Read activity reports for your organization	Yes	✓ Granted for Hanman ...
ActivityReports.Read	Application	Read activity reports for your organization	Yes	✓ Granted for Hanman ...
ServiceHealth.Read	Application	Read service health information for your organization	Yes	✓ Granted for Hanman ...
ThreatIntelligence.Read	Application	Read threat intelligence data for your organization	Yes	✓ Granted for Hanman ...
ThreatIntelligence.Read	Application	Read threat intelligence data for your organization	Yes	✓ Granted for Hanman ...

Configuration in FortiSIEM

Configuration is done in two parts. Follow the steps in these two sections to configure your FortiSIEM.

- Define Office 365 Management Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity

Define Office 365 Management Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Office365

Settings	Description
Access Protocol	Office 365 Mgmt Activity API
Tenant ID	Use the ID from Azure Login URL. See Step 5 in Create Office 365 API Credential.
Password config	If you select **Manual**, take the following steps: 1. For **Client ID**, use the value obtained in Step 5 in Create Office 365 API Credential. 2. For **Client Secret**, use the value obtained in Step 7 in Create Office 365 API Credential. For **CyberArk SDK** credential method, see CyberArk SDK Password Configuration. For **CyberARK REST API** credential method, see CyberArk REST API Password Configuration.
Authentication Endpoint	Enter the authentication endpoint. The Authentication Endpoint depends on the type of Office 365 environment you have: • Enterprise plan: login.windows.net • GCC government plan: login.microsoftonline.com • GCC High government plan: login.microsoftonline.us • DoD government plan: login.microsoftonline.us **Note**: Do NOT include "https://" in the **Authentication Endpoint** URL field.
Authentication Protocol	Enter the token location. For example, `/oauth2/token`.
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps.

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new association.
    a. Select the name of the credential created in the **Define Office 365 Management Credential** from the **Credentials** drop-down list.
    b. In the **IP/Host Name** field, enter the API Endpoint based off your Office 365 plan type. Your options are:
        - Enterprise plan: manage.office.com
        - GCC government plan: manage-gcc.office.com
        - GCC High government plan: manage.office365.us
        - DoD government plan: manage.protection.apps.mil

c. Click **Save**.

2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling. A pop up will appear and show the Test Connectivity results.
3. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Office 365 Log Collection.

Sample Events for Audit

```
[OFFICE365_EVENT_DATA] = {"Actor":[{"ID":"dtomic@my.company.org","Type":5},
{"ID":"10030000873CEE9F","Type":3},{"ID":"18ed3507-a475-4ccb-b669-d66bc9f2a36e","Type":2},
{"ID":"User_68d76168-813d-4b9f-88cd-37b66a5b3841","Type":2},
{"ID":"68d76168-813d-4b9f-88cd-37b66a5b3841","Type":2},
{"ID":"User","Type":2}],"ActorContextId":"653e32e8-fb2d-41aa-8841-90f05b340318","ActorIpAddr
ess":"<null>","AzureActiveDirectoryEventType":1,"ClientIP":"<null>","CreationTime":"2019-07-
23T13:16:05UTC","ExtendedProperties":
[{"Name":"actorContextId","Value":"653e32e8-fb2d-41aa-8841-90f05b340318"},
{"Name":"actorObjectId","Value":"68d76168-813d-4b9f-88cd-37b66a5b3841"},
{"Name":"actorObjectClass","Value":"User"},
{"Name":"actorUPN","Value":"dtomic@my.company.org"},
{"Name":"actorAppID","Value":"18ed3507-a475-4ccb-b669-d66bc9f2a36e"},
{"Name":"actorPUID","Value":"10030000873CEE9F"},{"Name":"teamName","Value":"MSODS."},
{"Name":"targetContextId","Value":"653e32e8-fb2d-41aa-8841-90f05b340318"},
{"Name":"targetObjectId","Value":"02232019-4557-45d6-9630-f78694bc8341"},
{"Name":"extendedAuditEventCategory","Value":"Application"},
{"Name":"targetName","Value":"FSM"},{"Name":"targetIncludedUpdatedProperties","Value":"
[\"AppAddress\",\"AppId\",\"AvailableToOtherTenants\",\"DisplayName\",\"RequiredResourceAcce
ss\"]"},{"Name":"correlationId","Value":"a854ecc6-31d6-4fea-8d56-aeed05aa1174"},
{"Name":"version","Value":"2"},{"Name":"additionalDetails","Value":"{}"},
{"Name":"resultType","Value":"Success"},
{"Name":"auditEventCategory","Value":"ApplicationManagement"},
{"Name":"nCloud","Value":"<null>"},{"Name":"env_ver","Value":"2.1"},{"Name":"env_
name","Value":"#Ifx.AuditSchema#IfxMsods.AuditCommonEvent"},{"Name":"env_
time","Value":"2019-07-23T13:16:05.0208099Z"},{"Name":"env_epoch","Value":"64BOV"},
{"Name":"env_seqNum","Value":"25454285"},{"Name":"env_popSample","Value":"0"},{"Name":"env_
iKey","Value":"ikey"},{"Name":"env_flags","Value":"257"},{"Name":"env_
cv","Value":"##17a913a8-943a-42f3-b8ad-2ea3bc4bf927_00000000-0000-0000-0000-000000000000_
17a913a8-943a-42f3-b8ad-2ea3bc4bf927"},{"Name":"env_os","Value":"<null>"},{"Name":"env_
osVer","Value":"<null>"},{"Name":"env_appId","Value":"restdirectoryservice"},{"Name":"env_
appVer","Value":"1.0.11219.0"},{"Name":"env_cloud_ver","Value":"1.0"},{"Name":"env_cloud_
name","Value":"MSO-AM5R"},{"Name":"env_cloud_role","Value":"restdirectoryservice"},
{"Name":"env_cloud_roleVer","Value":"1.0.11219.0"},{"Name":"env_cloud_
roleInstance","Value":"AM5RRDSR582"},{"Name":"env_cloud_environment","Value":"PROD"},
{"Name":"env_cloud_
deploymentUnit","Value":"R5"}],"Id":"fc12de96-0cbc-4618-9c8f-cc8ab7891e3b","ModifiedProperti
es":[{"Name":"AppAddress","NewValue":"[\r\n {\r\n \"AddressType\": 0,\r\n \"Address\":
\"https://10.222.248.17\",\r\n \"ReplyAddressClientType\": 1\r\n }\r\n]","OldValue":"[]"},
{"Name":"AppId","NewValue":"[\r\n
\"0388f2da-dbcc-4506-ba57-a85c578297c0\"\r\n]","OldValue":"[]"},
{"Name":"AvailableToOtherTenants","NewValue":"[\r\n false\r\n]","OldValue":"[]"},
{"Name":"DisplayName","NewValue":"[\r\n \"FSM\"\r\n]","OldValue":"[]"},
{"Name":"RequiredResourceAccess","NewValue":"[\r\n {\r\n \"ResourceAppId\":
\"00000003-0000-0000-c000-000000000000\",\r\n \"RequiredAppPermissions\": [\r\n {\r\n
\"EntitlementId\": \"e1fe6dd8-ba31-4d61-89e7-88639da4683d\",\r\n \"DirectAccessGrant\":
false,\r\n \"ImpersonationAccessGrants\": [\r\n 20\r\n ]\r\n }\r\n ],\r\n
\"EncodingVersion\": 1\r\n }\r\n]","OldValue":"[]"},{"Name":"Included Updated
Properties","NewValue":"AppAddress, AppId, AvailableToOtherTenants, DisplayName,
RequiredResourceAccess","OldValue":""}],"ObjectId":"Not Available","Operation":"Add
application.","OrganizationId":"653e32e8-fb2d-41aa-8841-90f05b340318","RecordType":8,"Result
Status":"Success","SupportTicketId":"","Target":[{"ID":"Application_
02232019-4557-45d6-9630-f78694bc8341","Type":2},
{"ID":"02232019-4557-45d6-9630-f78694bc8341","Type":2},{"ID":"Application","Type":2},
{"ID":"FSM","Type":1}],"TargetContextId":"653e32e8-fb2d-41aa-8841-90f05b340318","TenantId":"
653e32e8-fb2d-41aa-8841-90f05b340318","UserId":"dtomic@my.company.org","UserKey":"1003000087
3CEE9F@my.company.org","UserType":0,"Version":1,"Workload":"AzureActiveDirectory","phCustId"
:1}
```

Microsoft Cloud App Security

Integration Points

Protocol	Information Discovered	Used For
SIEM Agent	Logon, User creation/deletion and other Audit activity for Azure Applications including Office 365, SharePoint, OneDrive, Teams, PowerBI , Exchange	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "MS-Azure-CloudAppSec" in the **Search** field to see the event types associated with Microsoft Cloud App Security.

Configuring a SIEM Agent

FortiSIEM integrates with Microsoft Cloud App Security to collect alerts and activities from apps to Microsoft Cloud. As new activities and events are supported by connected apps, they become available to FortiSIEM via Microsoft Cloud App Security integration.

The integration is done via the Microsoft Cloud App Security SIEM agent. It can run on any server (including FortiSIEM). It pulls alerts and activities from Microsoft Cloud App Security and then streams them into FortiSIEM.

For details, see here.

FortiSIEM integration is accomplished in three steps:

1. Set up a SIEM Agent in the Microsoft Cloud App Security portal.
2. Download the SIEM agent (JAR file) and run it on a server. The agent would connect to the portal, collect logs and forward to FortiSIEM. The server could be a FortiSIEM node such as Collector.
3. Validate that the SIEM agent is working correctly.
4. Configure an application to connect to Microsoft Cloud App Security portal. See those events in FortiSIEM.

Step 1: Set Up a SIEM Agent in the Microsoft Cloud App Security Portal

1. In the Cloud App Security portal, under the Settings cog, click **Security extensions** and then click on the **SIEM agents** tab.
2. Click the plus icon to start the **Add SIEM agent** wizard.

3. In the wizard:
   a. Click **Start Wizard**.
   b. Fill in a name.
   c. **Select your SIEM format** as 'Generic CEF'.
   d. In **Advanced settings**:
      i. Set **Time Format** to 'RFC 5424'.
      ii. Check **Include PRI**.
      iii. Check **Include system name**.
   e. Click **Next**.
   f. Type in the IP address or hostname Forti**SIEM** node receiving the events and port **514**. Select TCP or UDP as the **SIEM** protocol. In most common situations, you would choose a FortiSIEM Collector. Click **Next**.
   g. Select which data types, **Alerts** and **Activities** you want to export to your **FortiSIEM**. **We recommend choosing All Alerts and All Activities**. You can use the Apply to drop-down to set filters to send only specific alerts and activities. You can click **Edit and preview results** to check that the filter works as expected. Click **Next**.
   h. The wizard will say that SIEM agent configuration is finished. Copy the token and save it for later.
   i. After you click **Finish** and leave the Wizard, back in the SIEM page, you can see the SIEM agent you added in the table. It will show that it's **Created** until it’s connected later.

Step 2: Download the SIEM agent (JAR file) and Run it on a Server

1. In the Microsoft Download Center, after accepting the software license terms, download the .zip file and unzip it.
2. Run the following command:

```
java -jar mcas-siemagent-0.87.20-signed.jar --logsDirectory <DIRNAME> --token <TOKEN> &
```

   where:
   - `DIRNAME` (optional) is the path to the directory for agent to write debug log.
   - `TOKEN` is the SIEM agent token you copied in the previous Step 1 Sub-step 3.h.

Step 3: Validate that the SIEM Agent is Working Correctly

Make sure the status of the SIEM agent in the Cloud App Security portal is 'Connected'.

If the connection is down for more than two hours, then the status may show 'Connection error'. The status will be 'Disconnected' if down for more than 12 hours.

Step 4: Configure an Application to Connect to Microsoft Cloud App Security Portal

Cloud App Security currently supports the following Office 365 apps:

- Office 365
- Dynamics 365 CRM
- Exchange (only appears after activities from Exchange are detected in the portal and requires you to turn on auditing)
- OneDrive
- PowerBI (only appears after activities from PowerBI are detected in the portal, and requires you to turn on auditing)
- SharePoint
- Teams (only appears after activities from Teams are detected in the portal)

See the Microsoft documentation to setup these applications.

Connecting Office 365 to Cloud App Security

Use the app connector API to connect Microsoft Cloud App Security to your existing Microsoft Office 365 account. The Microsoft Cloud App Security connection gives you visibility into and control over Office 365 use.

For information on how Cloud App Security helps protect your Office 365 environment, see here.

For information on the prerequisites and steps to connect Microsoft Cloud App Security to your existing Microsoft Office 365 account, see How to connect Office 365 to Cloud App Security.

Sample Events

```
<109>2018-05-22T04:17:28.340Z SP204 CEF:0|MCAS|SIEM_Agent|0.123.162|EVENT_CATEGORY_
LOGIN|Log
on|0|externalId=70e988af3b82e19b872d12a91860d300d968f47e0bb245a0e765d9dbfbdb02ce
rt=1526962648340 start=1526962648340 end=1526962648340 msg=Log on
suser=yanlong@shashiaccelops.onmicrosoft.com destinationServiceName=Microsoft Azure
dvc=43.254.220.13 requestClientApplication=;Windows 10;Edge 17.17134;
cs1Label=portalURL
cs1=https://shashiaccelops.us2.portal.cloudappsecurity.com/#/audits?activity.id\=eq
(70e988af3b82e19b872d12a91860d300d968f47e0bb245a0e765d9dbfbdb02ce,)
cs2Label=uniqueServiceAppIds cs2=APPID_AZURE cs3Label=targetObjects cs3=Azure
Portal,yanlong,yanlong cs4Label=policyIDs cs4= c6a1Label="Device IPv6 Address" c6a1=
```

Microsoft Defender for Identity (Previously Microsoft Azure Advanced Threat Protection (ATP))

- Integration Points
- Event Types
- Configuration
- Sample Event

Integration Points

Protocol	Information Discovered	Used For
Syslog (CEF)	Suspicious alerts occurring on Windows machine in Azure	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "MS-AzureATP" in the **Search** field to see the event types associated with Microsoft Azure Advanced Threat Protection (ATP).

Configuration

FortiSIEM receives alerts via CEF formatted syslog. See here for details.

Sample Event

```
02-21-2018 16:20:21 Auth.Warning 192.168.0.220 1 2018-02-21T14:20:06.156238+00:00
CENTER CEF 6076 LdapBruteForceSecurityAlert 0|Microsoft|Azure
ATP|2.22.4228.22540|LdapBruteForceSecurityAlert|Brute force attack using LDAP simple
bind|5|start=2018-02-21T14:19:41.7422810Z app=Ldap suser=Wofford Thurston shost=CLIENT1
msg=A brute force attack using the Ldap protocol was attempted on Wofford Thurston
(Software Engineer) from CLIENT1 (100 guess attempts). cnt=100 externalId=2004
cs1Label=url cs1=https://contoso-corp.atp.azure.com/securityAlert/57b8ac96-7907-4971-
9b27-ec77ad8c029a
```

Microsoft Azure Compute

- Configuration

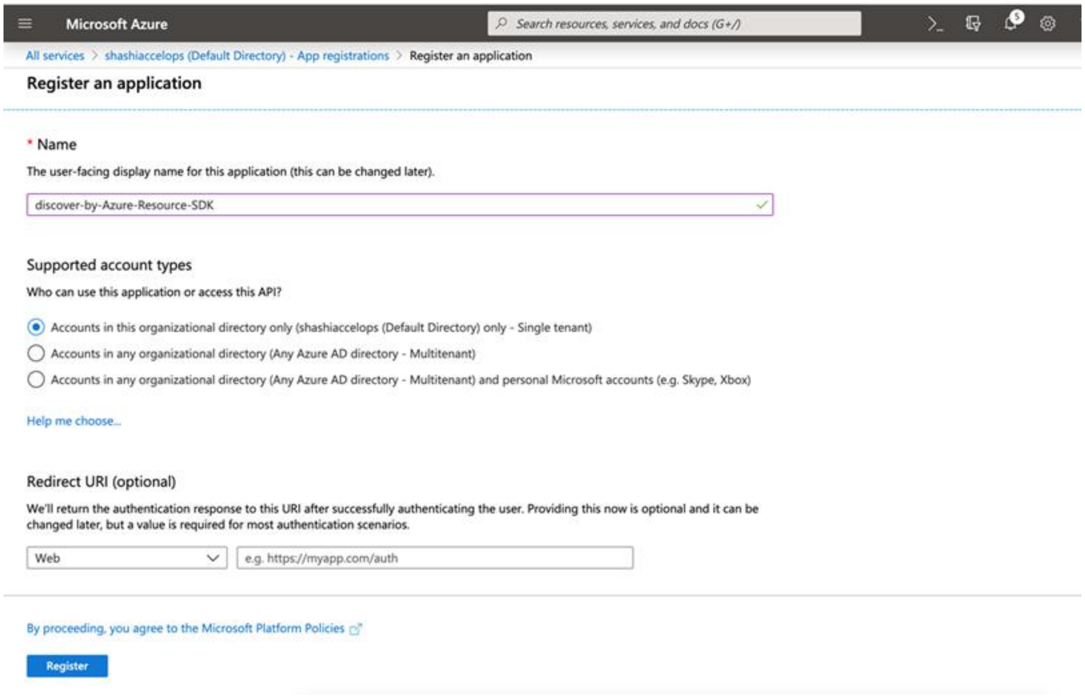
The purpose of this integration is to discover Virtual Machines (VMs) running in Azure. It does not collect events or performance statistics. Many Azure specific reports rely on properly categorizing which VMs exist in Azure Cloud. Please follow the appropriate integration guide for each instance in Azure you would like to ingest logs and monitor.

Configuration

- Setup in Azure
- Setup in FortiSIEM

Setup in Azure

1. Log in to the Azure Portal
2. Create an Azure Active Directory application
   - Sign in to your Azure Account through the Azure portal.
   - Select **Azure Active Directory**.
   - Select **App registrations**.
   - Select **New registration**.



Microsoft Azure
Search resources, services, and docs (G+/)
All services > shashiaccelops (Default Directory) - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

discover-by-Azure-Resource-SDK

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (shashiaccelops (Default Directory) only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

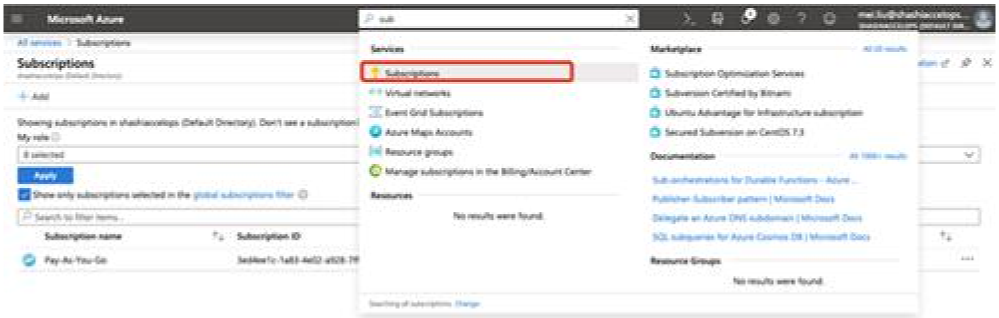
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

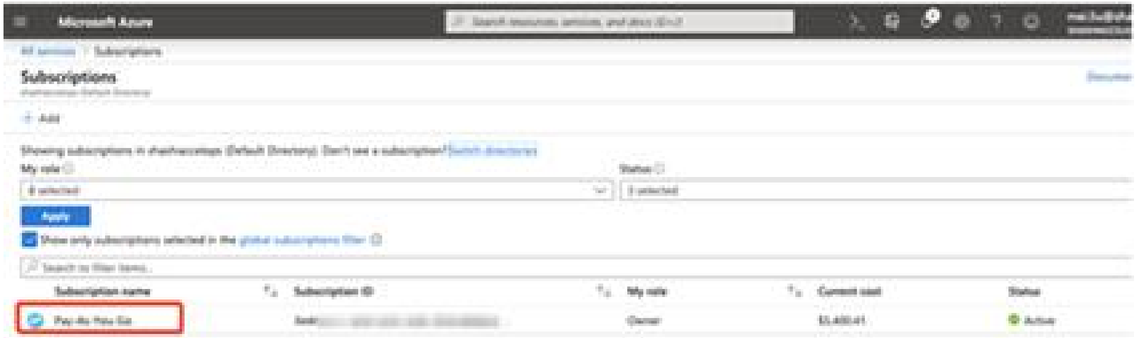
By proceeding, you agree to the Microsoft Platform Policies

3. Assign the application to a role:
   - Select **Subscriptions** on the Home page.

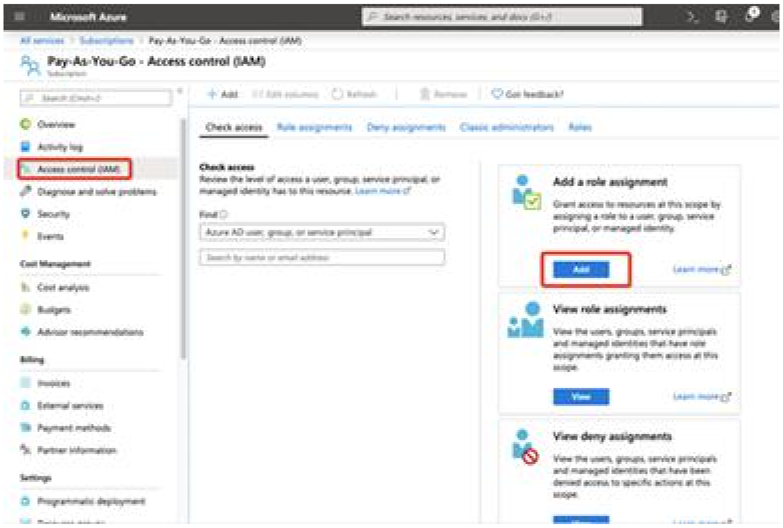


   - Select the particular subscription to assign your application to. In here, it uses Pay-As-You-GO as the example.

     Click Pay-AS-You-GO to open it. Save the **Subscription ID** for FortiSIEM credential.

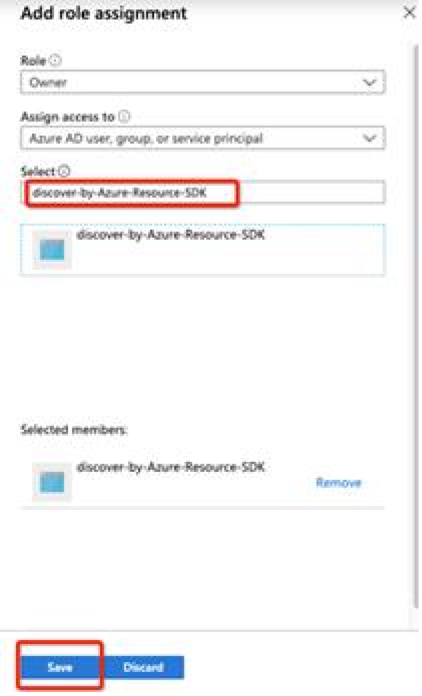


   - Copy the **Subscription ID**, it will be needed when defining the credential in FortiSIEM.
   - Select **Access control (IAM)**.



   - Select **Add role assignment**.

- Select **Owner** to assign to the application and select the app that you created. And then click **Save**.



Add role assignment

Role: Owner

Assign access to: Azure AD user, group, or service principal

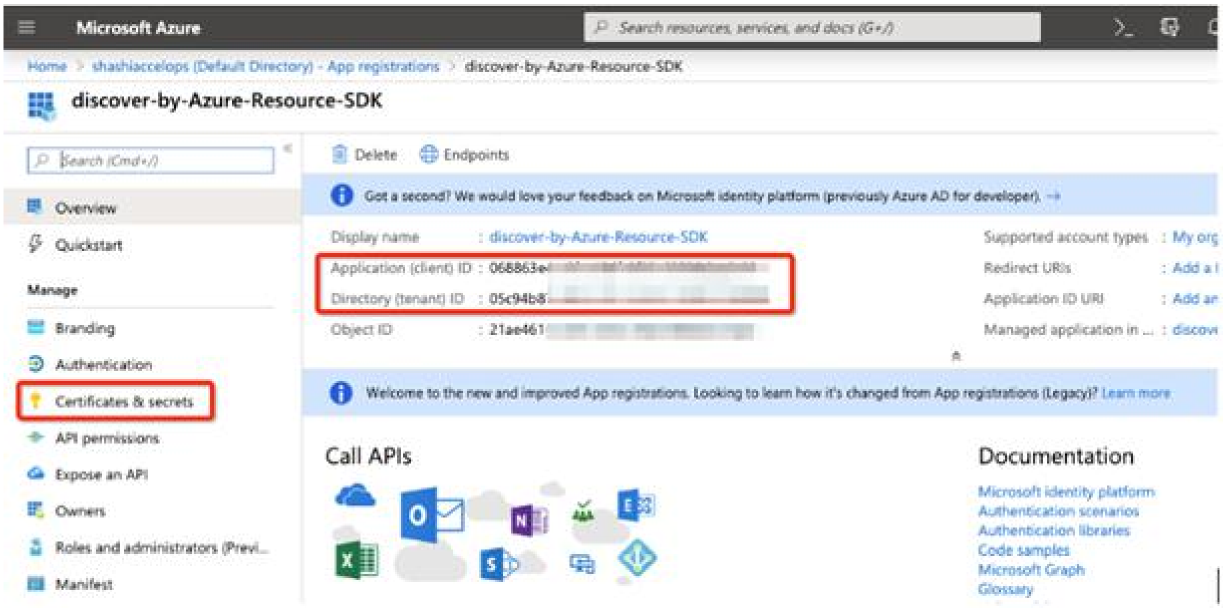
Select: discover-by-Azure-Resource-SDK

discover-by-Azure-Resource-SDK

Selected members:

discover-by-Azure-Resource-SDK Remove

4. Get value for FortiSIEM credential
   - Select **Azure Active Directory**.
   - From App registrations in Azure AD, select your application.



Microsoft Azure

Home > shashiaccelops (Default Directory) - App registrations > discover-by-Azure-Resource-SDK

discover-by-Azure-Resource-SDK

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : discover-by-Azure-Resource-SDK

Application (client) ID : 068863e[redacted]

Directory (tenant) ID : 05c94b8[redacted]

Object ID : 21ae461[redacted]

Supported account types : My org

Redirect URIs : Add a r

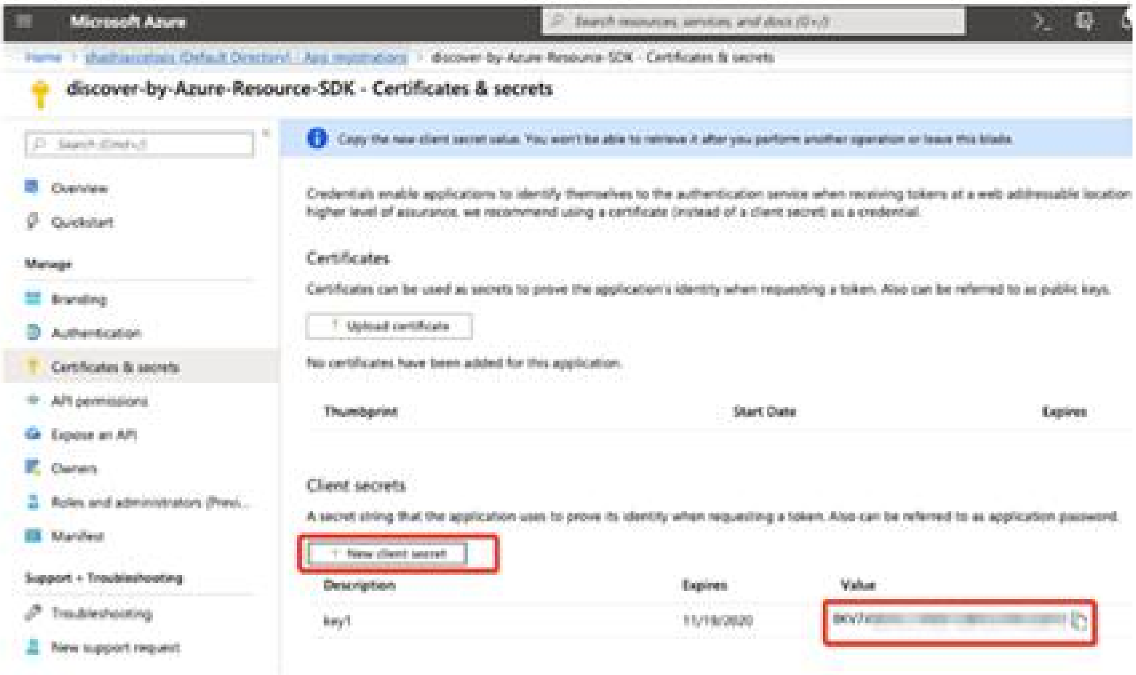
Application ID URI : Add an

Managed application in ... : discov

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

- Copy the **Application (client) ID** and **Directory (tenant) ID**, it will be needed when defining the credential in FortiSIEM.

- Select Certificate & secrets to generate a secret key.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > [illegible] (Default Directory) | App registrations > discover-by-Azure-Resource-SDK - Certificates & secrets
Search (Cmd+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Upload certificate
New client secret

discover-by-Azure-Resource-SDK - Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location
higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

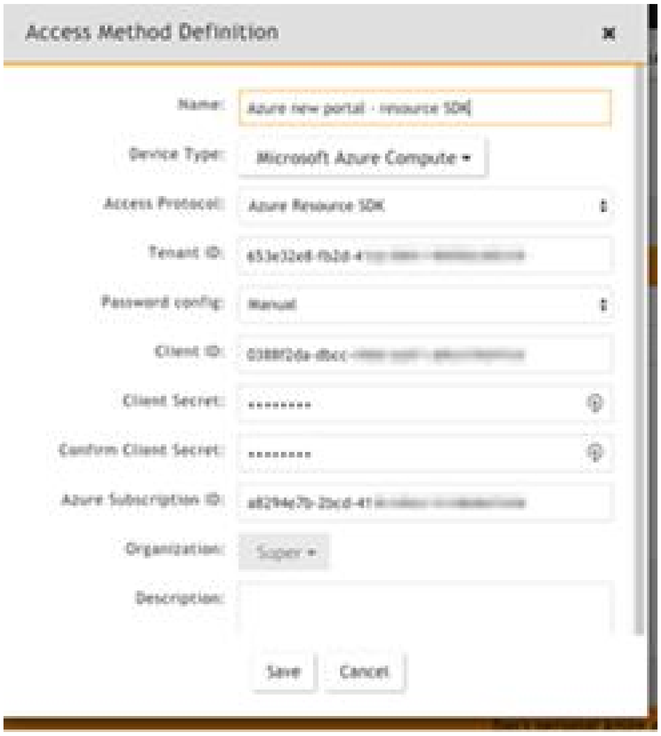
Description	Expires	Value
key1	11/18/2020	[redacted]

5. Test
   - Command:
     `/opt/phoenix/bin/getAzureResourceVM.py {subscriptionId} {tenantId} {clientId} {client secret}.`
   - Example:
     `/opt/phoenix/bin/getAzureResourceVM.py 7327432-1a83-4e02-a928-9032489032898a 05c94b87-da0c-4e11-be1d-789234789432 068863e4-c2fa-48df-8f33-79823478932 jh23hjkb324ugih32hujdsdsvqeP]]'`

Setup in FortiSIEM

Follow these steps in the FortiSIEM UI:

1. Create a new credential. Make sure to select **Azure Resource SDK** as the **Access Protocol**.



Access Method Definition

Name: Azure new portal - resource SDK

Device Type: Microsoft Azure Compute

Access Protocol: Azure Resource SDK

Tenant ID: 653e32e8-fb2d-4[redacted]

Password config: Manual

Client ID: 0388f2da-dbcc-[redacted]

Client Secret: ••••••••

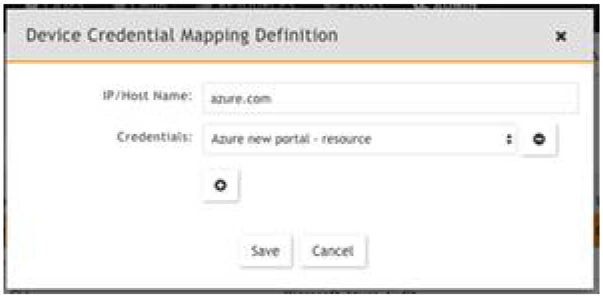
Confirm Client Secret: ••••••••

Azure Subscription ID: a8294e7b-2bcd-41[redacted]

Organization: Super

Description:

2. Define a credential.

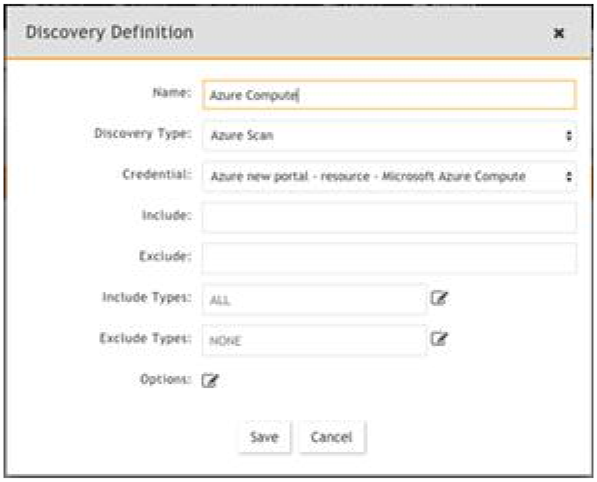


Device Credential Mapping Definition

IP/Host Name: azure.com

Credentials: Azure new portal - resource

3. Create a **Discovery Definition**.



Discovery Definition

Name: Azure Compute

Discovery Type: Azure Scan

Credential: Azure new portal - resource - Microsoft Azure Compute

Include:

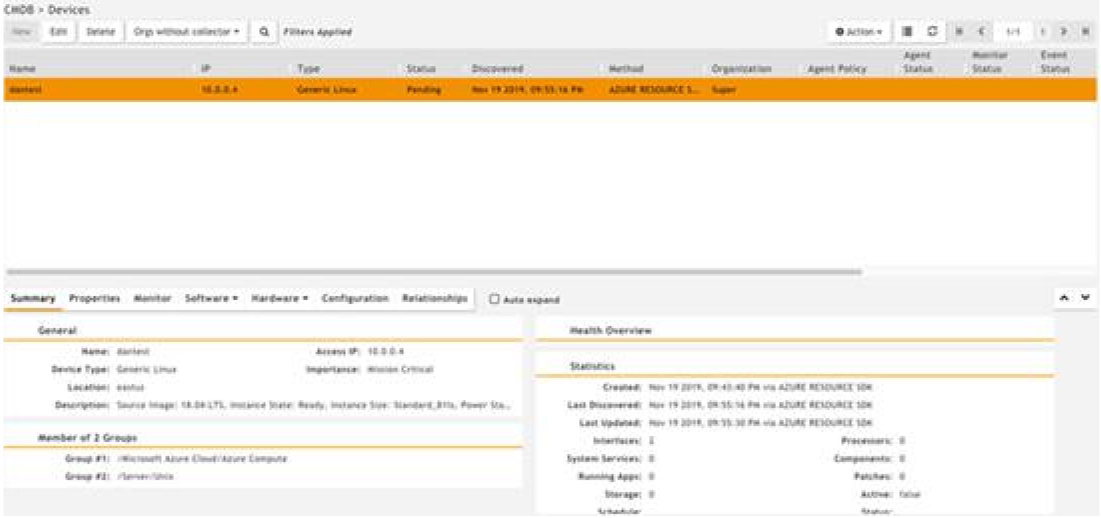
Exclude:

Include Types: ALL

Exclude Types: NONE

Options:

4. The CMDB should then be populated.



Name	IP	Type	Status	Discovered	Method	Organization	Agent Policy	Agent Status	Monitor Status	Event Status
dantest	10.0.0.4	Generic Linux	Pending	Nov 19 2019, 09:55:16 PM	AZURE RESOURCE S...	Super				

General

Name: dantest
Access IP: 10.0.0.4
Device Type: Generic Linux
Importance: Mission Critical
Location: eastus
Description: Source Image: 18.04-LTS, Instance State: Ready, Instance Size: Standard_B1s, Power Sta...

Member of 2 Groups

Group #1: /Microsoft Azure Cloud/Azure Compute
Group #2: /Server/Unix

Health Overview

Statistics

Created: Nov 19 2019, 09:43:40 PM via AZURE RESOURCE SDK
Last Discovered: Nov 19 2019, 09:55:16 PM via AZURE RESOURCE SDK
Last Updated: Nov 19 2019, 09:55:30 PM via AZURE RESOURCE SDK
Interfaces: 2
Processors: 0
System Services: 0
Components: 0
Running Apps: 0
Patches: 0
Storage: 0
Active: false
Scheduler:
Status:

Microsoft Azure Event Hub

Event Hubs is a fully managed, real-time data ingestion service that is simple, trusted, and scalable. Stream millions of events per second from any source to build dynamic data pipelines and immediately respond to business challenges.

Why might you use Azure Event Hubs with FortiSIEM?

You can aggregate all your custom log sources and telemetry data to Azure Event Hubs, which FortiSIEM can then ingest and process provided there is a FortiSIEM parser created for those custom log sources.

Although FortiSIEM already ingests Azure audit logs via another integration, Azure has an option to send diagnostic Audit logs to Azure Event Hub, that FortiSIEM can then ingest.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub

You can also export Azure monitoring data to an event hub: -- See section “Monitoring Data Available” for information on log types that can be exported to Azure Event Hub.

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/stream-monitoring-data-event-hubs

FortiSIEM uses the Azure Python SDK to integrate logs from the event hub to perform comprehensive security analysis. Azure Log Integration simplifies the task of integrating Azure logs with your on-premises SIEM system. The recommended method for integrating Azure logs is to stream the logs into event hubs via the Azure Monitor. FortiSIEM provides a connector to further integrate logs from the event hub into the SIEM.

Azure produces extensive logging for each Azure service. The logs represent these log types:

- **Control/management logs**: Provide visibility into the Azure Resource Manager CREATE, UPDATE, and DELETE operations. An Azure activity log is an example of this type of log.
- **Data plane logs**: Provide visibility into events that are raised when you use an Azure resource. An example of this type of log is the Windows Event Viewer's System, Security, and Application channels in a Windows virtual machine. Another example is Azure Diagnostics logging, which you configure through Azure Monitor.
- **Processed events**: Provide analyzed event and alert information that are processed for you. An example of this type of event is Azure Security Center alerts. Azure Security Center processes and analyzes your subscription to provide alerts that are relevant to your current security posture.

For more information on how to stream any type of log to an event hub, see:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/stream-monitoring-data-event-hubs

- What is Discovered and Monitored
- Event Types
- Reports
- Rules
- Configuration in Azure
- Configuration in FortiSIEM
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Information Collected	Used For
Azure Python SDK	None	Audit Logs	Security Monitoring

Event Types

No defined event types.

Reports

No defined reports.

Rules

No defined rules.

Configuration in Azure

Create an Event Hub Namespace and Event Hub

Complete these steps in the Azure Portal:

Step 1: Create a Resource Group in Azure

A resource group is a logical collection of Azure resources. All resources are deployed and managed in a resource group. To create a resource group:

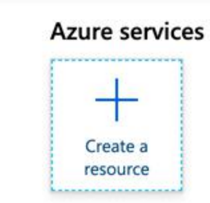
1. Login to the Azure portal: https://portal.azure.com/
2. Click **Resource groups** in the left navigation pane.
3. Click **Add**.
4. For **Subscription**, select the name of the Azure subscription in which you want to create the resource group.
5. Enter a unique name for the resource group, The system immediately checks to see if the name is available in the currently selected Azure subscription.
6. Select a **Region** for the resource group.
7. Click **Review + Create**.
8. Click **Create** on the **Review + Create** page.

Note: In the example used in step 2, a **Resource Group** called `fsm1` was created.

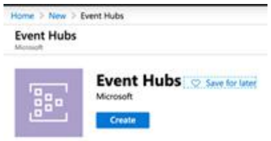
Step 2: Create an Event Hub Namespace

An Event Hub namespace provides a unique scoping container, referenced by its fully-qualified domain name, in which you create one or more event hubs. To create a namespace in your resource group using the portal, complete the following steps:

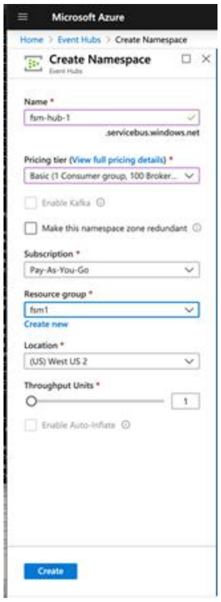
1. In the Azure portal, click **Create a resource** at the top left of the screen.



2. In the “**Search the Market** text box, enter **Select All services** in the left menu, select star (*) next to **Event Hubs**, and then click the **Create** button in the **ANALYTICS** category.



3. On the **Create namespace** page, complete the following steps:
    a. Enter a name for the namespace. The system immediately checks to see if the name is available.
    b. Choose the pricing tier **(Basic** or **Standard**).
    c. Select the subscription in which you want to create the namespace.
    d. Select a location for the namespace.
    e. Click **Create**. You may have to wait a few minutes for the system to fully provision the resources.



Name * fsm-hub-1 .servicebus.windows.net

Pricing tier (View full pricing details) * Basic (1 Consumer group, 100 Broker...

□ Enable Kafka

□ Make this namespace zone redundant

Subscription * Pay-As-You-Go

Resource group * fsm1

Create new

Location * (US) West US 2

Throughput Units * 1

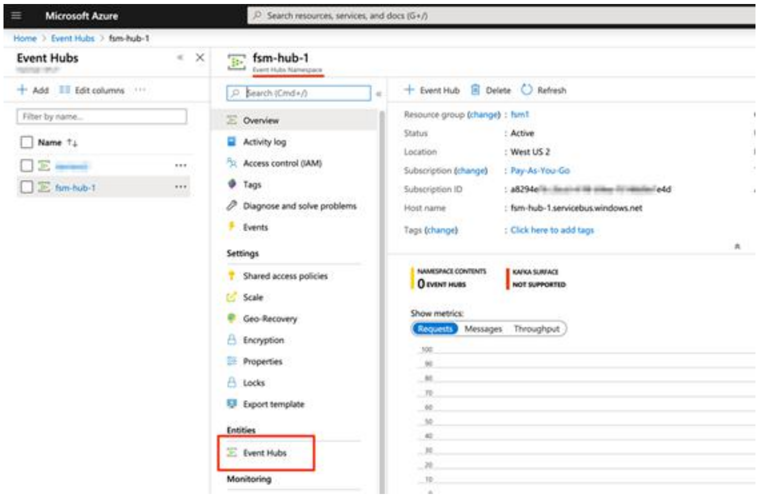
□ Enable Auto-Inflate

4. Refresh the **Event Hubs** page to see the event hub namespace. You can check the status of the event hub creation in the alerts.
5. Select the namespace. You see the home page for your **Event Hubs Namespace** in the portal.

Step 3: Create an Event Hub

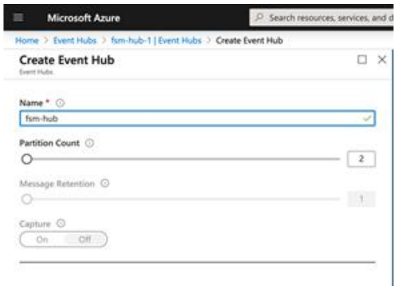
To create an event hub within the namespace, follow these steps:

1. In the **Event Hubs Namespace** page, click **Event Hubs** in the left menu.



Resource group (change) : fsm1
Status : Active
Location : West US 2
Subscription (change) : Pay-As-You-Go
Subscription ID : a8294e[redacted]e4d
Host name : fsm-hub-1.servicebus.windows.net
Tags (change) : Click here to add tags

2. At the top of the window, click **+ Event Hub**.
3. Enter a name for your event hub, then click **Create**.

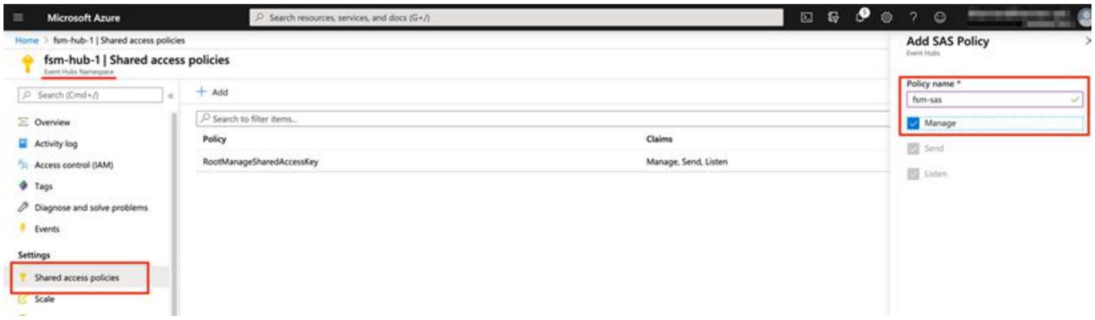

Microsoft Azure
Search resources, services, and d
Home > Event Hubs > fsm-hub-1 | Event Hubs > Create Event Hub
Create Event Hub
Event Hubs

Name * : fsm-hub
Partition Count : 2
Message Retention : 1
Capture : On Off

4. You can check the status of the event hub creation in alerts. After the event hub is created, you see it in the list of event hubs.

Step 4: Configure an Event Hub Namespace

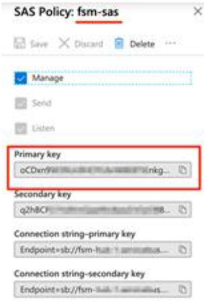
1. Select an event hub namespace and go to **Shared access policies**, and then click **+Add**. Enter the **Policy name**, check the **Manage** box, and then click **Create**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > fsm-hub-1 | Shared access policies
fsm-hub-1 | Shared access policies
Event Hubs Namespace
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events
Settings
Shared access policies
Scale
+ Add
Search to filter items...
Add SAS Policy
Event Hubs

Policy	Claims
RootManageSharedAccessKey	Manage, Send, Listen

Policy name * : fsm-sas
☑ Manage
☑ Send
☑ Listen

2. Select one of the **Shared Access** policies just created.
3. The Azure Python SDK needs the SAS **Policy name** (defined in step 4.1) and the **Primary key** when creating the credential in FortiSIEM. Copy the primary key and policy name to a text editor for later use.



SAS Policy: fsm-sas

☑ Manage

☑ Send

☑ Listen

Primary key

oCDxn[redacted]nkg...

Secondary key

q2hBCF[redacted]8...

Connection string–primary key

Endpoint=sb://fsm-[redacted]...

Connection string–secondary key

Endpoint=sb://fsm-[redacted]...

Note: When the event hub namespace is created, Azure will also create a default Shared Access Policy named **RootManageSharedAcessKey**.

4. Select an event hub namespace and go to **Event Hubs**.
5. Select an event hub and go to **Consumer** group. You can click **+Consumer group** or use default group name **$default**.

Note: If you have selected **Basic (1 Consumer Group)**, then there will be no option to add a another Consumer group.

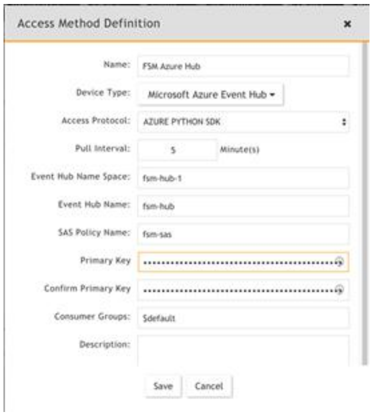
Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Azure Event Hub
Access Protocol	AZURE PYTHON SDK
Pull Interval	The interval in which FortiSIEM will pull events from Azure Event Hub. Default is 5 minutes.
Event Hub Namespace	The name of the Azure event hub namespace
Event Hub Name	The name of the Azure event hub.
SAS Policy Name	Shared Access (SAS) Policy Name
Primary Key	The name of the primary key
Consumer Group	The name of the consumer group
Description	Description of the device

Based on the example screenshots, this is the configuration in FortiSIEM:



Access Method Definition

Name: FSM Azure Hub

Device Type: Microsoft Azure Event Hub

Access Protocol: AZURE PYTHON SDK

Pull Interval: 5 Minute(s)

Event Hub Name Space: fsm-hub-1

Event Hub Name: fsm-hub

SAS Policy Name: fsm-sas

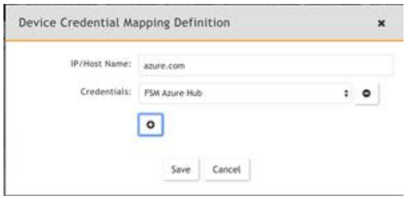
Primary Key ••

Confirm Primary Key ••

Consumer Groups: $default

Description:

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field. For this integration, enter "azure.com".
   b. Select the name of your Azure event hub credential from the **Credentials** drop-down list.
   c. Click **Save**.



Device Credential Mapping Definition

IP/Host Name: azure.com

Credentials: FSM Azure Hub

4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Azure event hub.
5. To see the jobs associated with Azure, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Azure" in the search box.

Note: Azure services must be configured to write to the Event Hub before there are any events to be collected.

Sample Events

```
{"records": [{ "count": 0, "total": 0, "minimum": 0, "maximum": 0, "average": 0,
"resourceId": "/SUBSCRIPTIONS/3ED4EE1C-1A83-4E02-A928-7FF5E0008E8A/RESOURCEGROUPS/ANDY_
TEST/PROVIDERS/MICROSOFT.EVENTHUB/NAMESPACES/FORTISIEMEVENTHUB", "time": "2019-02-
21T05:21:00.0000000Z", "metricName": "EHAMBS", "timeGrain": "PT1M"},{ "count": 0,
"total": 0, "minimum": 0, "maximum": 0, "average": 0, "resourceId":
"/SUBSCRIPTIONS/3ED4EE1C-1A83-4E02-A928-7FF5E0008E8A/RESOURCEGROUPS/ANDY_
TEST/PROVIDERS/MICROSOFT.EVENTHUB/NAMESPACES/FORTISIEMEVENTHUB", "time": "2019-02-
21T05:22:00.0000000Z", "metricName": "EHAMBS", "timeGrain": "PT1M"},{ "count": 0,
"total": 0, "minimum": 0, "maximum": 0, "average": 0, "resourceId":
"/SUBSCRIPTIONS/3ED4EE1C-1A83-4E02-A928-7FF5E0008E8A/RESOURCEGROUPS/ANDY_
TEST/PROVIDERS/MICROSOFT.EVENTHUB/NAMESPACES/FORTISIEMEVENTHUB", "time": "2019-02-
21T05:23:00.0000000Z", "metricName": "EHAMBS", "timeGrain": "PT1M"},{ "count": 0,
"total": 0, "minimum": 0, "maximum": 0, "average": 0, "resourceId":
"/SUBSCRIPTIONS/3ED4EE1C-1A83-4E02-A928-7FF5E0008E8A/RESOURCEGROUPS/ANDY_
TEST/PROVIDERS/MICROSOFT.EVENTHUB/NAMESPACES/FORTISIEMEVENTHUB", "time": "2019-02-
21T05:24:00.0000000Z", "metricName": "EHAMBS", "timeGrain": "PT1M"}]}
```

Microsoft Defender for Endpoint (Previously Microsoft Windows Defender Advanced Threat Protection (ATP))

- Integration Points
- Configuring Windows Defender for FortiSIEM REST API Access
- Configuring FortiSIEM for Windows Defender ATP REST API Access

Integration Points

Protocol	Information Discovered	Used For
Windows Defender API REST API		Security and Compliance

Configuring Windows Defender for FortiSIEM REST API Access

Microsoft provides ample documentation here.

Follow the steps specified in 'Enabling SIEM integration', repeated here.

1. Login to Windows Defender Center.
2. Go to **Settings** > **SIEM**.
3. Select **Enable SIEM integration**.
4. Choose **Generic API**.
5. Click **Save Details to File**.
6. Click **Generate Tokens**.

Configuring FortiSIEM for Windows Defender ATP REST API Access

Use the account in the previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

- Define Windows Defender ATP REST API Access Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity
- Viewing Events

Define Windows Defender ATP REST API Access Credential in FortiSIEM

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Microsoft Windows Defender ATP
Access Protocol	Windows Defender ATP Alert REST API
Tenant ID	Enter the Tenant ID for the credential created through the process here.
Password config	1. For **Manual**, enter the **Client ID** and **Client Secret** for the credential created here. For **CyberArk SDK**, see CyberArk SDK Password Configuration. For **CyberArk REST API**, see CyberArk REST API Password Configuration.
Organization	Choose an organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps.

1. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Depending on your region/business needs, enter one of the following into the **IP/Host Name** field.
      Note: Make sure to enter with `https://`.
      Enterprise:
      EU: https://wdatp-alertexporter-eu.windows.com/api/alerts
      US: https://wdatp-alertexporter-us.windows.com/api/alerts
      UK: https://wdatp-alertexporter-uk.windows.com/api/alerts

      GCC: https://wdatp-alertexporter-us.gcc.securitycenter.windows.us
      GCC High and DoD: https://wdatp-alertexporter-us.securitycenter.windows.us
   b. Select the name of the credential created in step 2 Configuring FortiSIEM for Windows Defender ATP REST API Access from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Windows Defender Center using the REST API.

Viewing Events

To view events received via Windows Defender ATP REST API, take the following steps:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the Windows Defender ATP entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from Windows Defender Center in the last 15 minutes. You can modify the time interval to get more events.

Okta

FortiSIEM can integrate with Okta as a single sign-on service for FortiSIEM users, discover Okta users and import them into the CMDB, and collect audit logs from Okta. See Setting Up External Authentication for information on configuring Okta to use as a single sign-on service, and Adding Users from Okta for discovering users and associating them with the Okta authentication profile. Once you have discovered Okta users, FortiSIEM will begin to monitor Okta events.

- What is Discovered and Monitored
- Event Types
- Configuration
- Access Credentials in FortiSIEM
- Sample Okta Event
- Adding Users from Okta
- Configuring Okta Authentication
- Logging In to Okta
- Setting Up External Authentication

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Okta API			

Event Types

In **ADMIN > Device Support > Event Types**, search for "okta" to see the event types associated with this device.

Configuration

- In Okta **Administartion -> Security -> API**, create a token. Note, tokens generated by this mechanism will have the permissions of the user who generated them.
- Tokens are valid for 30 days and automatically refresh with each API call. Tokens that are not used for 30 days will expire. The token lifetime is currently fixed and cannot be changed.

Access Credentials in FortiSIEM

Setting	Value
Name	<name>
Device Type	OKTA.com OKTA
Access Protocol	OKTA API

Setting	Value
Pull Interval	5
Domain	The name of your OKTA domain
Security Token	The token that has been created in Okta
Organization	Select an organization from the drop-down list.

Sample Okta Event

```
Mon Jul 21 15:50:26 2014 FortiSIEM-Okta [action/message]=Sign-in successful
[action/objectType]=core.user_auth.login_success [action/requestUri]=/login/do-login
[actors/0/displayName]=CHROME [actors/0/id]=Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36
[actors/0/ipAddress]=211.144.207.10 [actors/0/login]=YaXin.Hu@accelops.com
[actors/0/objectType]=Client [eventId]=tev-UlpTnWJRI2vXNRKTJHE4A1405928963000
[eventName]=USER-AUTH-LOGIN-SUCCESS [published]=2014-07-21T07:49:23.000Z
[requestId]=U8zGA0zxVNXabfCeka9oGAAAA [sessionId]=s024bi4GPUkRaegPXuA1IFEDQ
[targets/0/displayName]=a_name [targets/0/id]=00uvdkhrxcPNGYWISAGK [targets/0/login]=a_
name@doamin.com [targets/0/objectType]=User
```

Adding Users from Okta

- Create an Okta API Token
- Define Okta Credential and Associate It with an IP Address
- Discover Okta Users

Create an Okta API Token

1. Log in to Okta using your Okta credentials.
2. Got to **Administration > Security > API Tokens**.
3. Click **Create Token**.
   You will use this token when you set up the Okta login credentials in the next section. Note that this token will have the same permissions as the person who generated it.

Define Okta Credential and Associate It with an IP Address

Take the following steps from these sections:

- Define Okta Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity

Define Okta Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**. Your LDAP credentials will be added after clicking **Save**.

1.

Settings	Description
Name	Enter a name for the credential
Device Type	OKTA.com OKTA
Access Protocol	OKTA API
Pull Interval	Enter how often, in minutes, you want FortiSIEM to pull information from Okta.
Domain	Enter the **NetBIOS/Domain** associated with your Okta account. For example, `FortiSIEM.okta.com`
Security Token	Enter the security token information.
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps.

1. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter the IP range or host name for your Okta account in the **IP/Host Name** field.
   b. Select your Okta credentials from the **Credentials** drop-down list created in Define Okta Credential in FortiSIEM step 2a.
   c. Click **Save**. Your Okta credentials will appear in the list of credential/IP address associations in **Step 2: Enter IP Range to Credential Associations.**
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity** to make sure you can connect to the Okta server. A pop up will appear and show the Test Connectivity results.

Discover Okta Users

If the number of users are less than 200, then Test Connectivity will discover all the users.

Okta API has some restrictions that does not allow FortiSIEM to pull more than 200 users. In this case, follow these steps:

1. Login to **Okta**.
2. Download user list CSV file (OktaPasswordHealth.csv) from **Admin** > **Reports** > **Okta Password Health**.
3. Rename the CSV file to `all_user_list_%s.csv` (where `%s` is the placeholder of token obtained in Create an Okta API Token - Step 3, for example, `all_user_list_00UbCrgrU9b1Uab0cHCuup-5h-6Hi9ItokVDH8nRRT.csv`).

4. Login to **FortiSIEM Supervisor node**:
   a. Upload csv file `all_user_list_%s.csv` to this directory `/opt/phoenix/config/okta/`
   b. Make sure the permissions are admin and admin (Run "`chown -R admin:admin /opt/phoenix/config/okta/`")
   c. Go to **ADMIN > Setup > Credentials**, and in **Step 2: Enter IP Range to Credential Associations**, select the Okta entry, click on the **Test** drop-down list and select **Test Connectivity** to import all users.

Configuring Okta Authentication

To use Okta authentication for your FortiSIEM deployment, you must set up a SAML 2.0 Application in Okta, and then use the certificate associated with that application when you configure external authentication.

1. Log in to Okta.
2. In the **Applications** tab, create a new application using **Template SAML 2.0 App**.
3. Under **Settings**, configure the settings similar to the table below:

Post Back URL	Post Back URL
Application label	FortiSIEM Demo
Force Authentication	Enable
Post Back URL	https://<FortiSIEMIP>/phoenix/okta
Name ID Format	EmailAddress
Recipient	FortiSIEM
Audience Restriction	Super
authnContextClassRef	PasswordProtectedTransport
Response	Signed
Assertion	Signed
Request	Uncompressed
Destination	https://<FortiSIEMIP>/phoenix/okta

4. Click **Save**.
5. In the **Sign On** tab, click **View Setup Instructions**.
6. Click **Download Certificate**.
7. Enter the downloaded certificate for Okta authentication.

Logging In to Okta

Follow these steps to log in to Okta from the Okta domain `https://fortinetfsm.okta.com`. You cannot log into Okta from the FortiSIEM UI.

1. Create a new Okta account from `https://www.okta.com/` or log in to an existing account, using the domain `fortinetfsm.okta.com`.
2. Configure users for the account, for example, `testone@fortinet.com`, `testtwo@fortinet.com`, and so on. See Adding Users From Okta and Create Login Credentials and Associate Them with an IP Address.
3. Discover the Okta users to ensure that you have users to test. See Discover Okta Users.

4. Create a SAML authentication configuration from Okta based on the OKTA SAML 2.0 template. See Configuring Okta Authentication.
5. Associate the users (for example, `testone@fortinet.com` and `testtwo@fortinet.com`) to the external profile in **CMDB > Users**.
6. Log in to the Okta domain `https://fortinetfsm.okta.com` as one of the users you defined in Step 2.
7. Click the SAML configuration application in Okta (see Configuring Okta Authentication). You can now log in to Okta.

Setting Up External Authentication

You have three options for setting up external authentication for your FortiSIEM deployment: LDAP, RADIUS, and Okta.

Multiple Authentication Profiles

If more than one authentication profile is associated with a user, then the servers will be contacted one-by-one until a connection to one of them is successful. Once a server has been contacted, if the authentication fails, the process ends, and the user is notified that the authentication failed.

1. Log in to your Supervisor node.
2. Go to **ADMIN > Settings > General > External Authentication**.
3. Click **New**.
4. If you are setting up authentication for an organization within a multi-tenant deployment, select the **Organization**.
5. Select the **Protocol**.
6. Complete the protocol settings.

Protocol	User-Defined Settings
LDAP	Access IP Select Set DN Pattern to open a text field in which you can enter the DN pattern if you want to override the discovered pattern, or you want to add a specific LDAP user.
RADIUS	Access IP Shared Secret Select CHAP if you are using encrypted authentication to your RADIUS server. See also Juniper Networks Steel-Belted RADIUS.
Okta	Certificate See Configuring Okta Authentication for more information.

7. Click **Test**, and then enter credentials associated with the protocol you selected to make sure users can authenticate to your deployment.

Salesforce CRM Audit

- What is Discovered and Monitored
- Event Types
- Reports
- Configuration
- Sample Events for Salesforce Audit

What is Discovered and Monitored

Protocol	Logs Collected	Used For
Salesforce API	Successful/Failed Login, API Query Activity, Dashboard Activity, Opportunity Activity, Report Export Activity, Report Activity, Document Download Activity	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Salesforce Audit" in the **Search** field to see the event types associated with this device.

Reports

There are many reports defined in **RESOURCES > Reports > Device > Application > CRM**

- Salesforce Failed Logon Activity
- Salesforce Successful Logon Activity
- Top Browsers By Failed Login Count
- Top Browsers By Successful Login Count
- Top Salesforce Users By Failed Login Count
- Top Salesforce Users By Successful Login Count
- Top Successful Salesforce REST API Queries By Count, Run Time
- Top Failed Salesforce Failed REST API Queries By Count, Run Time
- Top Salesforce API Queries By Count, Run Time
- Top Salesforce Apex Executions By Count, Run Time
- Top Salesforce Dashboards Views By Count
- Top Salesforce Document Downloads By Count
- Top Salesforce Opportunity Reports By Count
- Top Salesforce Report Exports By Count
- Top Salesforce Reports By Count, Run Time
- Top Salesforce Events

Configuration

- Salesforce Configuration
- Define Salesforce Audit Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity

Salesforce Configuration

Salesforce saves events in a SQL Database, where FortiSIEM will pull the following events from tables: **EventLogFile**, **LoginHistory**,**User**, **Dashboard**, **Opportunity**, **Report** through SQL commands.

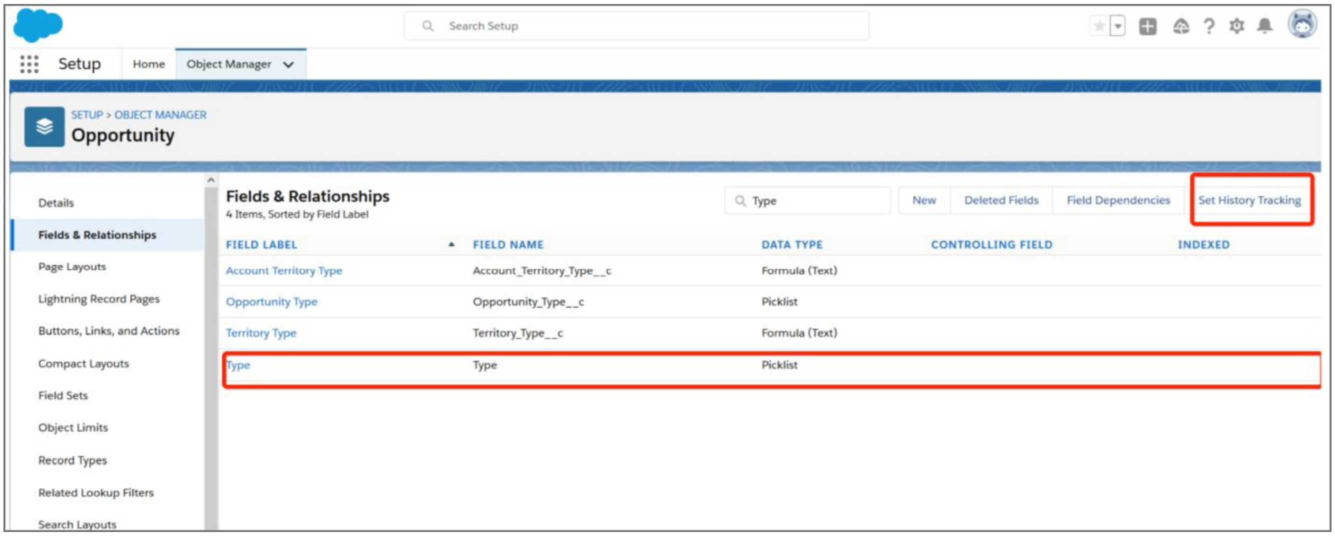
If you get an error about missing columns, please make sure your administrator has enabled **Set History Tracking** for the missing columns in the tables.

For more information on how to enable Set History Tracking, please refer to https://help.salesforce.com/articleView?id=sf.updating_picklists.htm&type=5

The required columns are listed in this table.

Event	Required Columns
EventLogFile	Id, EventType, LogFile, LogDate, LogFileLength, LastModifiedDate, LastModifiedDate
LoginHistory	Id, UserId, LoginTime, Browser, Platform, Status, SourceIp, LoginTime , LoginTime
Dashboard	Id, Description, DeveloperName, FolderName, Title, LastModifiedDate, LastModifiedDate LastModifiedDate
Opportunity	Id, Amount, CloseDate, Name, OwnerId, Type, LastModifiedDate, LastModifiedDate, LastModifiedDate
Report	Id, Name
User	Id, Username

For example, if Type in Opportunity is not enabled in Set History Tracking, FortiSIEM will fail to get events in Opportunity.



Search Setup

Setup | Home | Object Manager

SETUP > OBJECT MANAGER

Opportunity

- Details
- Fields & Relationships
- Page Layouts
- Lightning Record Pages
- Buttons, Links, and Actions
- Compact Layouts
- Field Sets
- Object Limits
- Record Types
- Related Lookup Filters
- Search Layouts

Fields & Relationships
4 Items, Sorted by Field Label

Type | New | Deleted Fields | Field Dependencies | Set History Tracking

FIELD LABEL	FIELD NAME	DATA TYPE	CONTROLLING FIELD	INDEXED
Account Territory Type	Account_Territory_Type__c	Formula (Text)		
Opportunity Type	Opportunity_Type__c	Picklist		
Territory Type	Territory_Type__c	Formula (Text)		
Type	Type	Picklist		

Define Salesforce Audit Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Salesforce Salesforce Audit
Access Protocol	Salesforce API
Pull Interval	5 minutes
Timeout	30 seconds
Password config	See Password Configuration
User Name	User name for device access
Password	Password for device access
Security Token	Security token
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (From **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   1. Enter "login.salesforce.com" in the **IP/Host Name** field.
   2. Select the name of the credential created in the "Define Salesforce Audit Credential in FortiSIEM" from the **Credentials** drop-down list.
   3. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Salesforce Audit Log Collection.

Sample Events for Salesforce Audit

```
[Salesforce_Activity_Perf]:[activityType]=API,[activityName]=get_user_info,
[srcIpAddr]=23.23.13.166,[user]=huiping.hp@gmail.com,[deviceTime]=1458112097,
[isSuccess]=false,[runTime]=31,[cpuTime]=9,[dbTime]=19434051,[infoURL]=Api
```

Console Access Devices

FortiSIEM supports this console access device for discovery and monitoring.

- Lantronix SLC Console Manager

Lantronix SLC Console Manager

- What is Discovered and Monitored
- Event Types
- Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Admin access, Updates, Commands run	Log analysis and compliance

Event Types

The complete list of Lantronix SLC log event types can be found in **ADMIN > Device Support > Event Types** by searching for "Lantronix-SLC". Some important ones are:

- Lantronix-SLC-RunCmd
- Lantronix-SLC-Update
- Lantronix-SLC-User-Logon-Success

Configuration

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example Syslog

```
<174>xmsd: gen/info-Syslog server changed to 10.4.3.37
<38>xwsd[32415]: auth/info-Web Authentication Success for user andbr003
```

End Point Security Software

The following anti-virus and host security (HIPS) applications are supported for discovery and monitoring by FortiSIEM.

- Bit9 Security Platform
- Carbon Black Security Platform
- Cisco AMP for Endpoints API V0 - Previously Cisco AMP Cloud V0
- Cisco AMP for Endpoints API V1 - Previously Cisco AMP Cloud V1
- Cisco Security Agent (CSA)
- CloudPassage Halo
- CrowdStrike Endpoint Security
- Digital Guardian Code Green DLP
- ESET NOD32 Anti-Virus
- FortiClient
- FortinetFortiEDR
- Malwarebytes Breach Remediation
- MalwareBytes Endpoint Protection
- McAfee ePolicy Orchestrator (ePO)
- MobileIron Sentry and Connector
- Netwrix Auditor
- Palo Alto Traps Endpoint Security Manager
- SentinelOne
- Sophos Central
- Sophos Endpoint Security and Control
- Symantec Endpoint Protection
- Symantec SEPM
- Tanium Connect
- Trend Micro Interscan Web Filter
- Trend Micro Intrusion Defense Firewall (IDF)
- Trend Micro OfficeScan

Bit9 Security Platform

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Bit9" to see the event types associated with this device.

Rules

- Bit9 Agent Uninstalled or File Tracking Disabled
- Bit9 Fatal Errors
- Blocked File Execution
- Unapproved File Execution

Reports

- Bit9 Account Group Changes
- Bit9 Fatal and Warnings Issues
- Bit9 Functionality Stopped
- Bit9 Security Configuration Downgrades

Bit9 Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<14>1 2015-04-06T16:24:02Z server1.foo.com - - - - Bit9 event:  text="Server discovered new
file 'c:\usersacct\appdata\local\temp\3cziegdd.dll'
[361aa7fbd5d00aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f]." type="Discovery"
subtype="New file on network" hostname="SVR123" username="SVR123\acct" date="4/6/2015
4:22:52 PM" ip_address="10.168.1.1" process="c:\abc\infrastructure\bin\scannerreset.exe"
file_path="c:\users\acct\appdata\local\temp\3cziegdd.dll" file_name="3cziegdd.dll" file_
hash="361aa7fbd5d00aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f" installer_
name="csc.exe" policy="High Enforce" process_key="00000000-0000-1258-01d0-7085edb50080"
server_version="7.2.0.1395" file_trust="-2" file_threat="-2" process_trust="-1" process_
threat="-1"
```

Carbon Black Security Platform

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Carbon Black Configuration
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Carbon Black" to see the event types associated with this device.

Rules

- Carbon Black Agent Uninstalled or File Tracking Disabled
- Carbon Black Fatal Errors
- Blocked File Execution
- Unapproved File Execution

Reports

- Carbon Black Account Group Changes
- Carbon Black Fatal and Warnings Issues
- Carbon Black Functionality Stopped
- Carbon Black Security Configuration Downgrades

Carbon Black Configuration

Syslog

The following guide should be used to install the python Carbon Black Cloud Syslog Connector on your FortiSIEM collector.

Note: You may need your Carbon Black account to view the Unix instructions.

https://developer.carbonblack.com/reference/carbon-black-cloud/integrations/syslog-connector/

An install guide with a sample configuration file is available here:

https://pypi.org/project/cbc-syslog/1.3.1/

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514. CEF formatted logs are also supported.

Sample Syslog

Standard Syslog:

```
<14>1 2015-04-06T16:24:02Z server1.foo.com - - - - Carbon Black event:  text="Server
discovered new file 'c:\usersacct\appdata\local\temp\3cziegdd.dll'
[361aa7fbd5d00aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f]." type="Discovery"
subtype="New file on network" hostname="SVR123" username="SVR123\acct" date="4/6/2015
4:22:52 PM" ip_address="10.168.1.1" process="c:\abc\infrastructure\bin\scannerreset.exe"
file_path="c:\users\acct\appdata\local\temp\3cziegdd.dll" file_name="3cziegdd.dll" file_
hash="361aa7fbd5d00aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f" installer_
name="csc.exe" policy="High Enforce" process_key="00000000-0000-1258-01d0-7085edb50080"
server_version="7.2.0.1395" file_trust="-2" file_threat="-2" process_trust="-1" process_
threat="-1
```

CEF Formatted Syslog:

```
<14>May 06 13:28:09 host1 CEF:0|Carbon Black|Protection|8.0.0.2562|809|Report write (custom
rule)|4|externalId=649219 cat=Policy Enforcement start=May 06 13:27:41 UTC rt=May 06
13:28:02 UTC filePath=c:\\windows\\system32\\perfdisk.dll fname=perfdisk.dll
fileHash=60b8a55c0f3228b18d918a3fd6684c401442f6447f2cec5dad9860a8c1d6462c fileId=39126
deviceProcessName="C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\4.14.17639.18041-
0\\MsMDEV.exe" dst=172.30.31.13 dhost=EXAMPLE\\DC01 duser=NT AUTHORITY\\SYSTEM
dvchost=cbprotection msg='c:\\windows\\system32\\perfdisk.dll' was created by 'NT
AUTHORITY\\SYSTEM'. sproc=00000000-0000-15b8-01d3-dd191e70c6d3 cs1Label=rootHash
cs1=e1c32fca51d86aad28c2dd13ec427eccd03f9d6900f8f1fe90b99f85550a8a98
cs2Label=installerFilename cs2=msi669d.tmp cs3Label=Policy cs3=Domain Controllers
cs5Label=ruleName cs5=[File Integrity Monitoring] Changes to system files
cfp1Label=fileTrust cfp1=10 flexString1Label=fileThreat flexString1=0 - Clean
cfp2Label=processTrust cfp2=10 flexString2Label=processThreat flexString2=0 - Clean
```

Cisco AMP for Endpoints API V0 - Previously Cisco AMP Cloud V0

- What is Discovered and Monitored
- Event Types
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Logs Collected	Used For
CloudAMP API	End point malware activity	Security Monitoring

Event Types

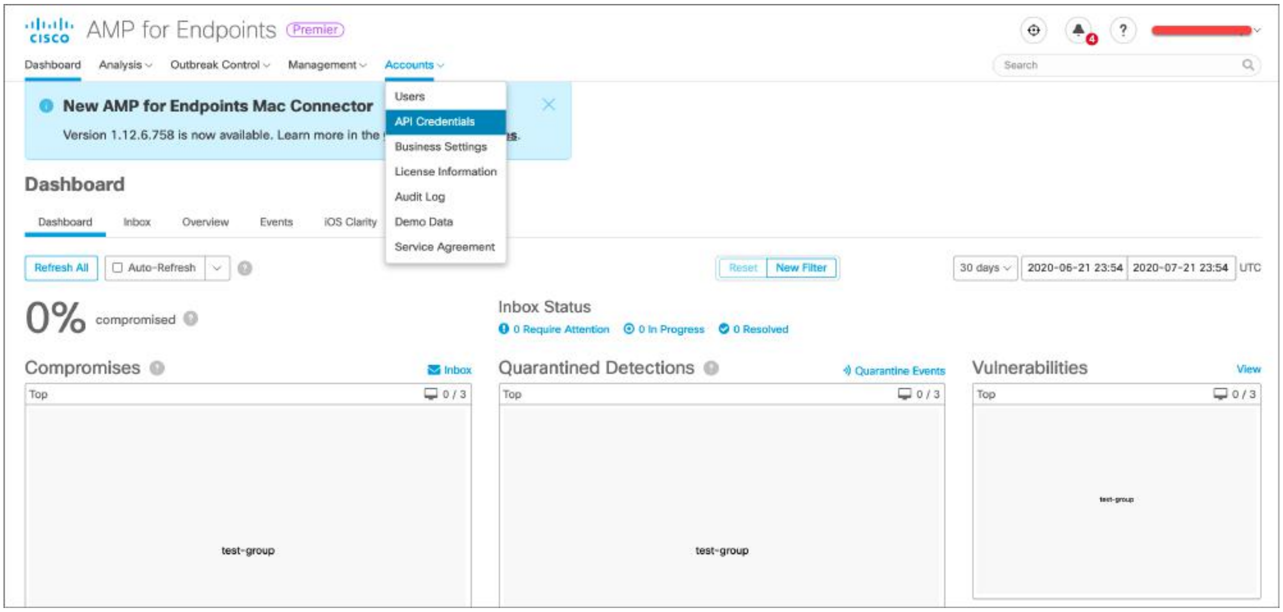
In **ADMIN > Device Support > Event Types**, search for "FireAMP Cloud" in the **Search** field to see the event types associated with this device.

Configuration

- Configure Cisco AMP Cloud V0
- Define Cisco FireAMP Cloud Credential in FortiSIEM
- Create IP Range to Credential Association, Test Connectivity, and Event Pulling

Configure Cisco AMP Cloud V0

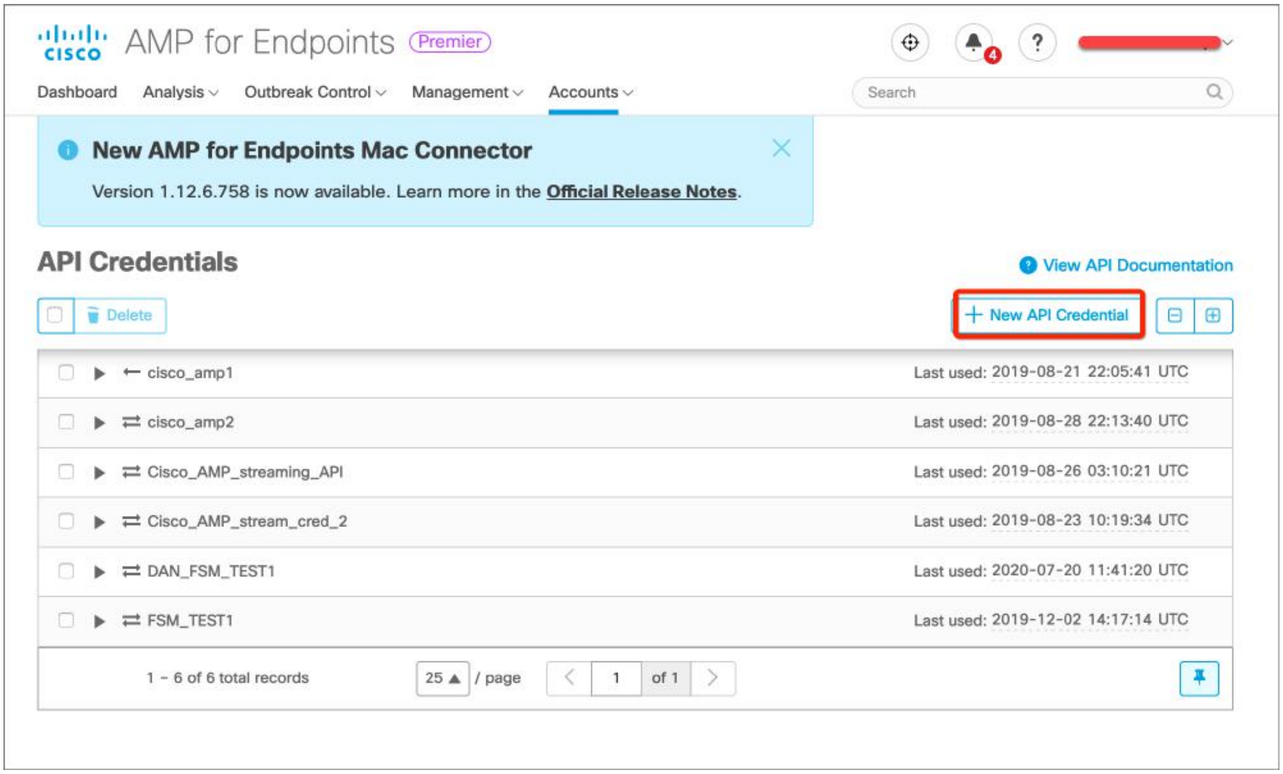
1. Login in https://auth.amp.cisco.com/.
2. Click **Accounts-> API Credentials**.



New AMP for Endpoints Mac Connector

Version 1.12.6.758 is now available. Learn more in the

3. Click **New API Credential**.



New AMP for Endpoints Mac Connector

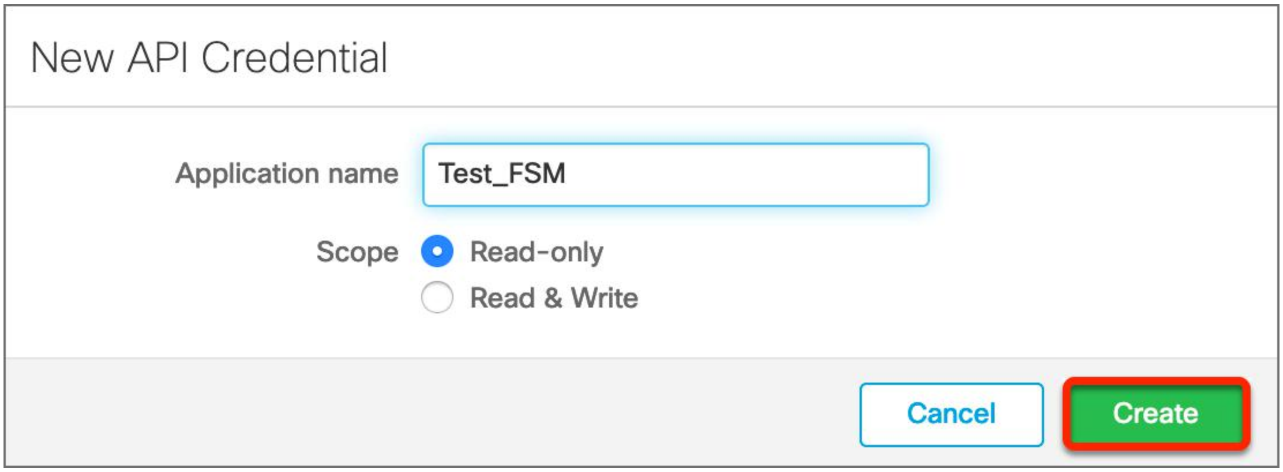
Version 1.12.6.758 is now available. Learn more in the **Official Release Notes**.

API Credentials

cisco_amp1	Last used: 2019-08-21 22:05:41 UTC
cisco_amp2	Last used: 2019-08-28 22:13:40 UTC
Cisco_AMP_streaming_API	Last used: 2019-08-26 03:10:21 UTC
Cisco_AMP_stream_cred_2	Last used: 2019-08-23 10:19:34 UTC
DAN_FSM_TEST1	Last used: 2020-07-20 11:41:20 UTC
FSM_TEST1	Last used: 2019-12-02 14:17:14 UTC

1 - 6 of 6 total records

4. Input **Application name** and click **Create**.

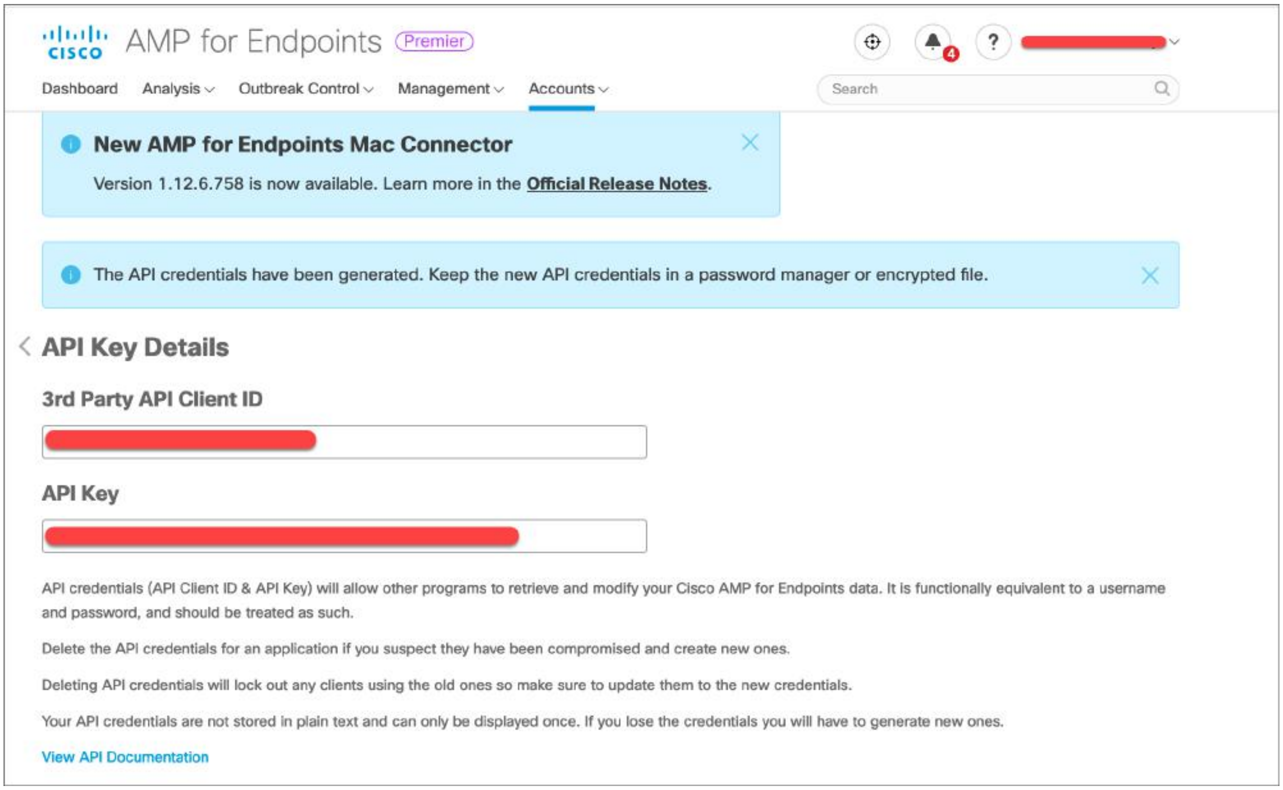


New API Credential

Application name: Test_FSM

Scope: ● Read-only ○ Read & Write

5. Record the **API Client ID** and **API key**. You will need them in a later step.



New AMP for Endpoints Mac Connector

Version 1.12.6.758 is now available. Learn more in the Official Release Notes.

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

API Key Details

3rd Party API Client ID: [redacted]

API Key: [redacted]

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

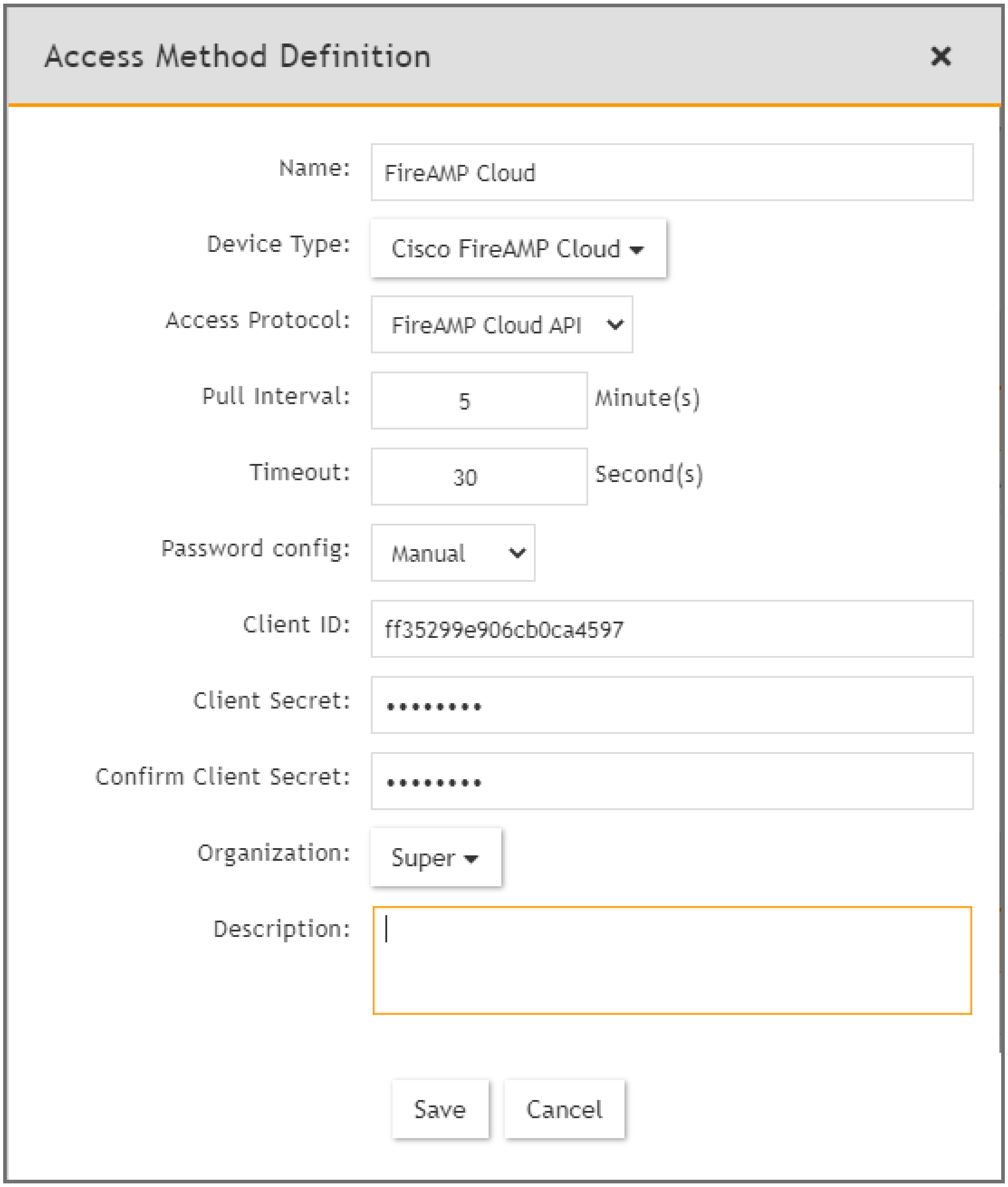
View API Documentation

Define Cisco FireAMP Cloud Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
1. b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, for example "FireAMP Cloud"
Device Type	Cisco FireAMP Cloud
Access Protocol	FireAMP Cloud API
Password config	Manual
Client ID	CiscoAMP Client ID
Client Secret	CiscoAMP API Key
Organization	The organization the device belongs to.
Description	Description of the device.



Access Method Definition

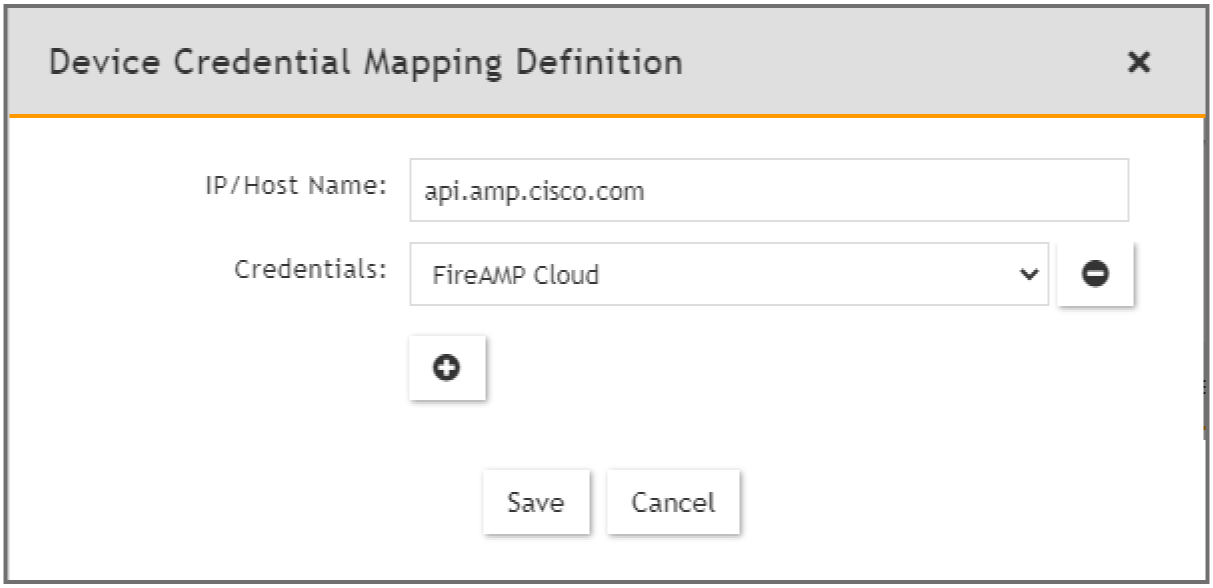
Name:	FireAMP Cloud
Device Type:	Cisco FireAMP Cloud
Access Protocol:	FireAMP Cloud API
Pull Interval:	5 Minute(s)
Timeout:	30 Second(s)
Password config:	Manual
Client ID:	ff35299e906cb0ca4597
Client Secret:	••••••••
Confirm Client Secret:	••••••••
Organization:	Super
Description:	

Create IP Range to Credential Association, Test Connectivity, and Event Pulling

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter "api.amp.cisco.com" in the **IP/Host Name** field.
   b. Select the name of the credential created in Define Cisco FireAMP Cloud Credential in FortiSIEM from the **Credentials** drop-down list.

c. Click **Save**.

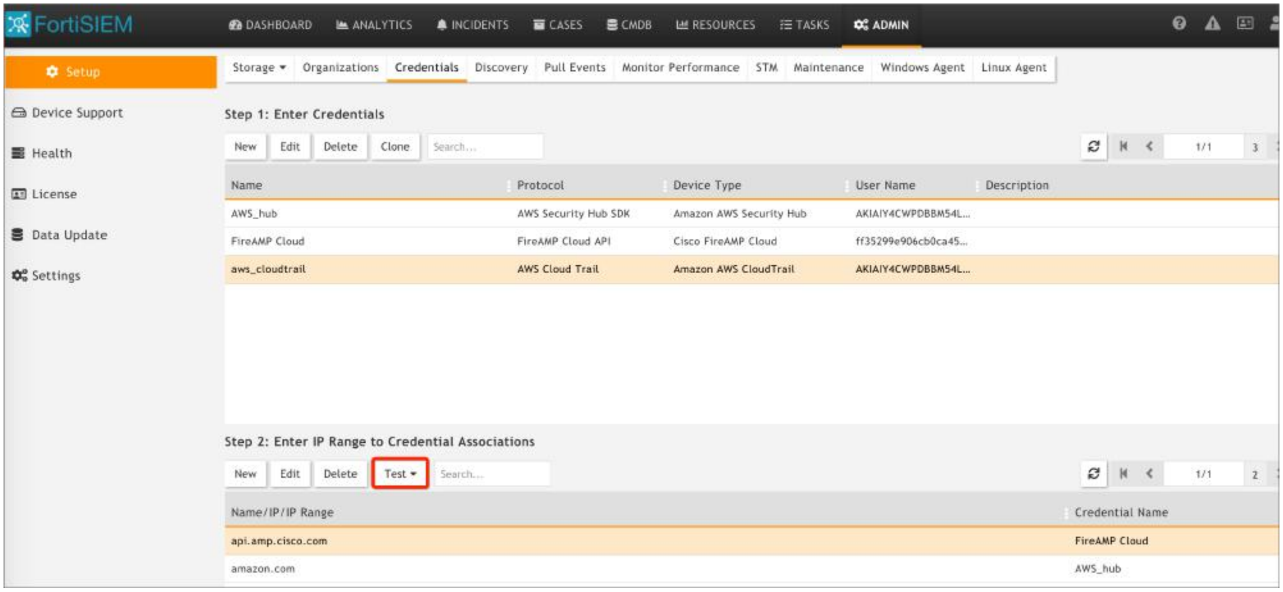


Device Credential Mapping Definition

IP/Host Name: api.amp.cisco.com

Credentials: FireAMP Cloud

2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity**. A pop up will appear and show the Test Connectivity results.



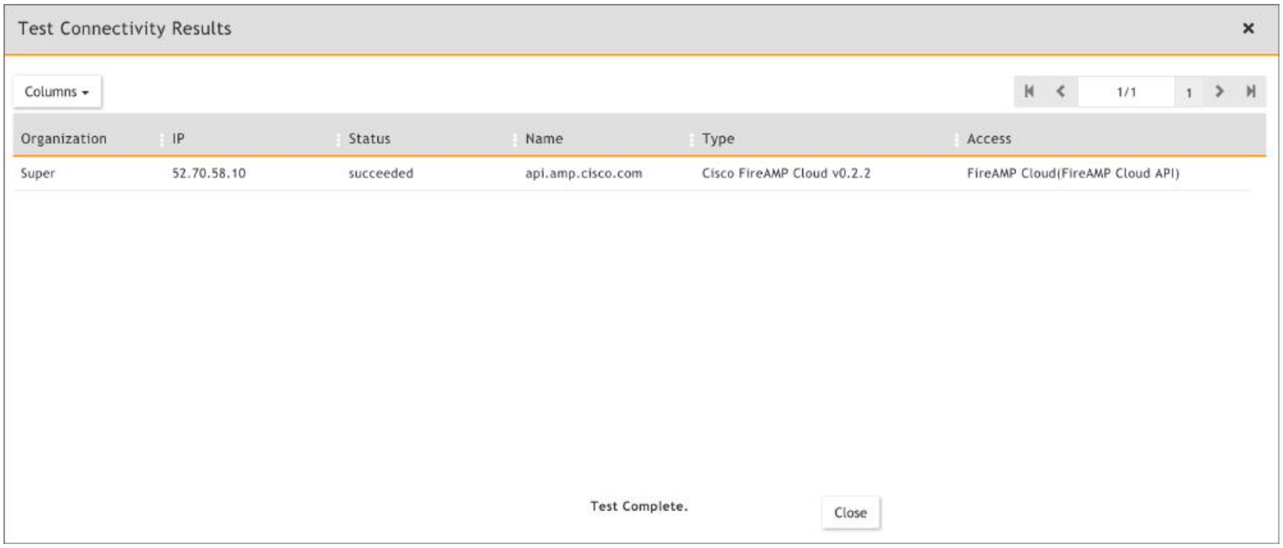
Step 1: Enter Credentials

Name	Protocol	Device Type	User Name	Description
AWS_hub	AWS Security Hub SDK	Amazon AWS Security Hub	AKIAIY4CWPDBBM54L...	
FireAMP Cloud	FireAMP Cloud API	Cisco FireAMP Cloud	ff35299e906cb0ca45...	
aws_cloudtrail	AWS Cloud Trail	Amazon AWS CloudTrail	AKIAIY4CWPDBBM54L...	

Step 2: Enter IP Range to Credential Associations

Name/IP/IP Range	Credential Name
api.amp.cisco.com	FireAMP Cloud
amazon.com	AWS_hub

The result is a success.

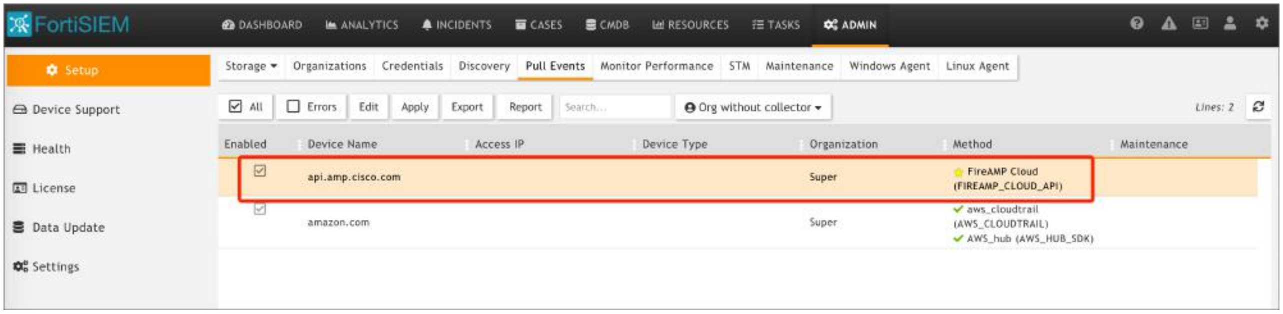


Test Connectivity Results

Organization	IP	Status	Name	Type	Access
Super	52.70.58.10	succeeded	api.amp.cisco.com	Cisco FireAMP Cloud v0.2.2	FireAMP Cloud(FireAMP Cloud API)

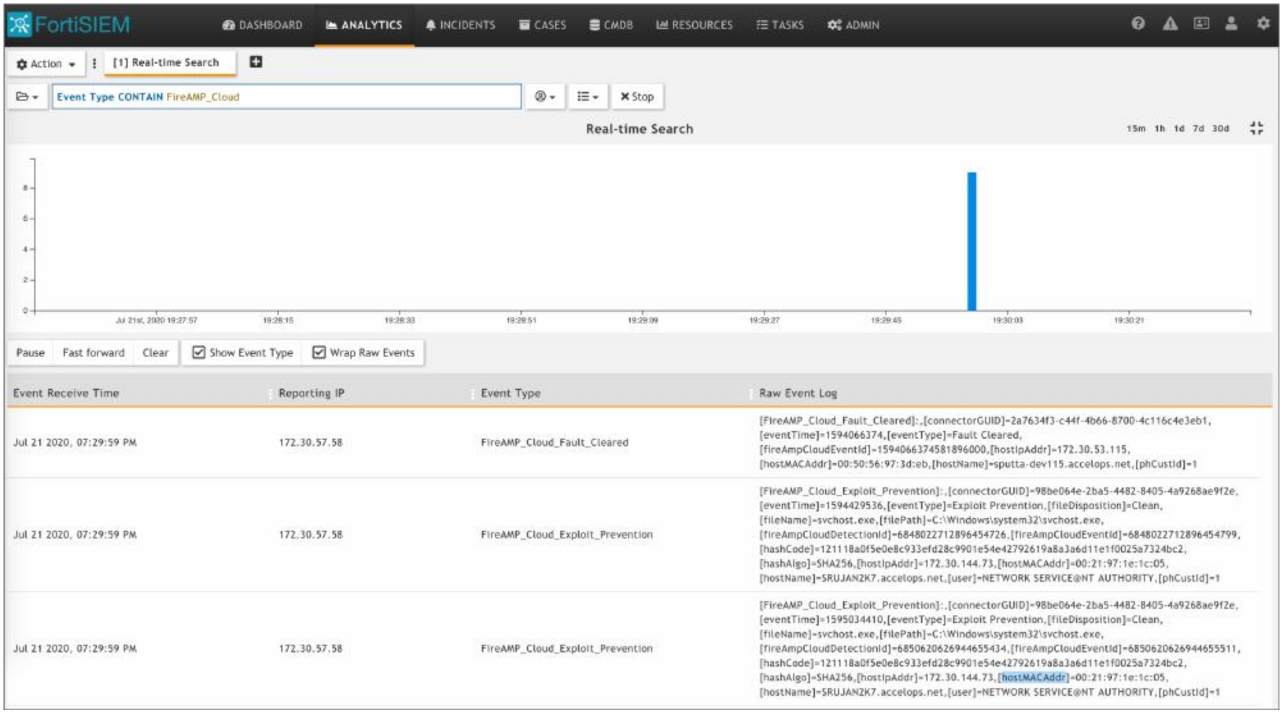
Test Complete.

3. Go to **ADMIN > Setup > Pull Events** and make sure an entry is created for Cisco FireAMP Cloud.



Enabled	Device Name	Access IP	Device Type	Organization	Method	Maintenance
☑	api.amp.cisco.com			Super	FireAMP Cloud (FIREAMP_CLOUD_API)	
☑	amazon.com			Super	✓ aws_cloudtrail (AWS_CLOUDTRAIL) ✓ AWS_hub (AWS_HUB_SDK)	

4. Go to the **ANALYTICS** page to see the events.



Event Type CONTAIN FireAMP_Cloud

Event Receive Time	Reporting IP	Event Type	Raw Event Log
Jul 21 2020, 07:29:59 PM	172.30.57.58	FireAMP_Cloud_Fault_Cleared	[FireAMP_Cloud_Fault_Cleared]:,[connectorGUID]=2a7634f3-c44f-4b66-8700-4c116c4e3eb1, [eventTime]=1594066374,[eventType]=Fault Cleared, [fireAmpCloudEventId]=1594066374581896000,[hostIpAddr]=172.30.53.115, [hostMACAddr]=00:50:56:97:3d:eb,[hostName]=sputta-dev115.accelops.net,[phCustId]=1
Jul 21 2020, 07:29:59 PM	172.30.57.58	FireAMP_Cloud_Exploit_Prevention	[FireAMP_Cloud_Exploit_Prevention]:,[connectorGUID]=98be064e-2ba5-4482-8405-4a9268ae9f2e, [eventTime]=1594429536,[eventType]=Exploit Prevention,[fileDisposition]=Clean, [fileName]=svchost.exe,[filePath]=C:\Windows\system32\svchost.exe, [fireAmpCloudDetectionId]=6848022712896454726,[fireAmpCloudEventId]=6848022712896454799, [hashCode]=121118a0f5e0e8c933efd28c9901e54e42792619a8a3a6d11e1f0025a7324bc2, [hashAlgo]=SHA256,[hostIpAddr]=172.30.144.73,[hostMACAddr]=00:21:97:1e:1c:05, [hostName]=SRUJAN2K7.accelops.net,[user]=NETWORK SERVICE@NT AUTHORITY,[phCustId]=1
Jul 21 2020, 07:29:59 PM	172.30.57.58	FireAMP_Cloud_Exploit_Prevention	[FireAMP_Cloud_Exploit_Prevention]:,[connectorGUID]=98be064e-2ba5-4482-8405-4a9268ae9f2e, [eventTime]=1595034410,[eventType]=Exploit Prevention,[fileDisposition]=Clean, [fileName]=svchost.exe,[filePath]=C:\Windows\system32\svchost.exe, [fireAmpCloudDetectionId]=6850620626944655434,[fireAmpCloudEventId]=6850620626944655511, [hashCode]=121118a0f5e0e8c933efd28c9901e54e42792619a8a3a6d11e1f0025a7324bc2, [hashAlgo]=SHA256,[hostIpAddr]=172.30.144.73,[hostMACAddr]=00:21:97:1e:1c:05, [hostName]=SRUJAN2K7.accelops.net,[user]=NETWORK SERVICE@NT AUTHORITY,[phCustId]=1

Sample Events

```
[FireAMP_Cloud_Threat_Detected]:[eventSeverity]=PHL_CRITICAL, [connectorGUID]=12345,
[date]=2015-11- 25T19:17:39+00:00,[detection]=W32.DFC.MalParent,
[detectionId]=6159251516445163587,[eventId]=6159251516445163587, [eventType]=Threat
Detected,[eventTypeId]=1090519054, [fileDispostion]=Malicious,[fileName]=rjtsbks.exe,
[fileSHA256]=3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370,
```

Cisco AMP for Endpoints API V1 - Previously Cisco AMP Cloud V1

Cisco Advanced Malware Protection (AMP) for Endpoints API V1 is a lightweight connector that can use the public cloud or be deployed as a private cloud, relying on AMQP Event Streams.

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configure Cisco AMP Cloud V1
- Configure FortiSIEM
- Sample Events

What is Discovered and Monitored

Protocol	Information collected	Used for
AMQP	Global threat intelligence, advanced sand boxing, and real-time malware blocking.	Intrusion protection system

Event Types

In **RESOURCES > Event Types**, enter "Cisco AMP" in the **Search** field to see the event types associated with this device.

Rules

No defined rules.

Reports

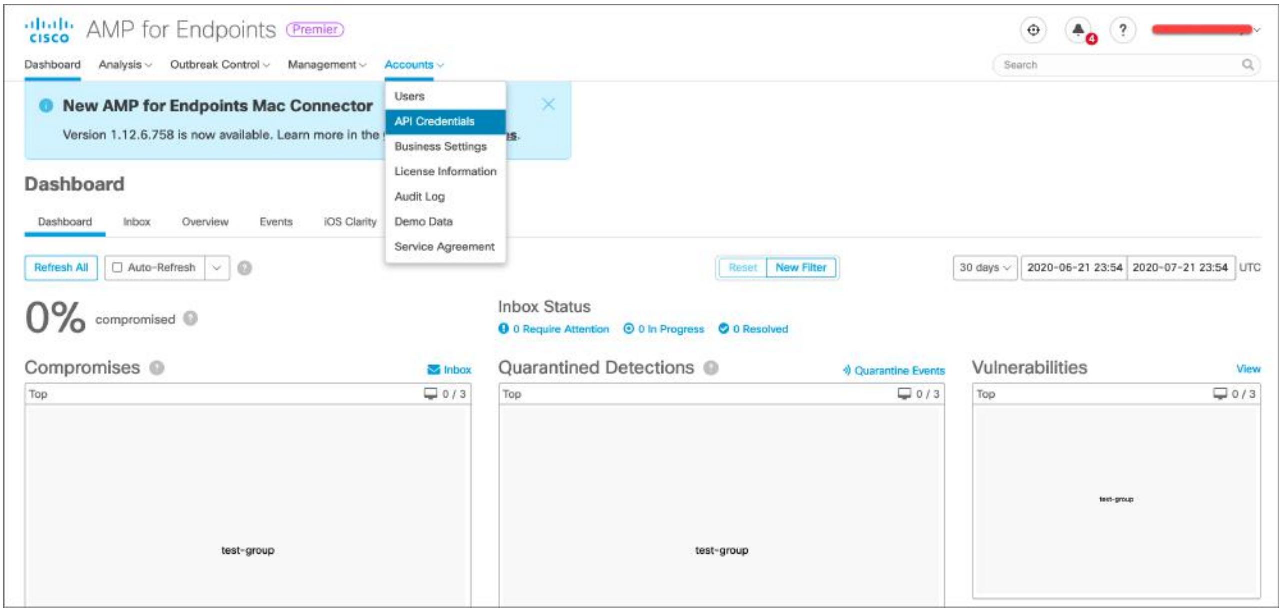
No defined reports.

Configuration

- Configure Cisco AMP Cloud V1
- Define Cisco CloudAMP Credential in FortiSIEM
- Create IP Range to Credential Association, Test Connectivity, and Event Pulling Check

Configure Cisco AMP Cloud V1

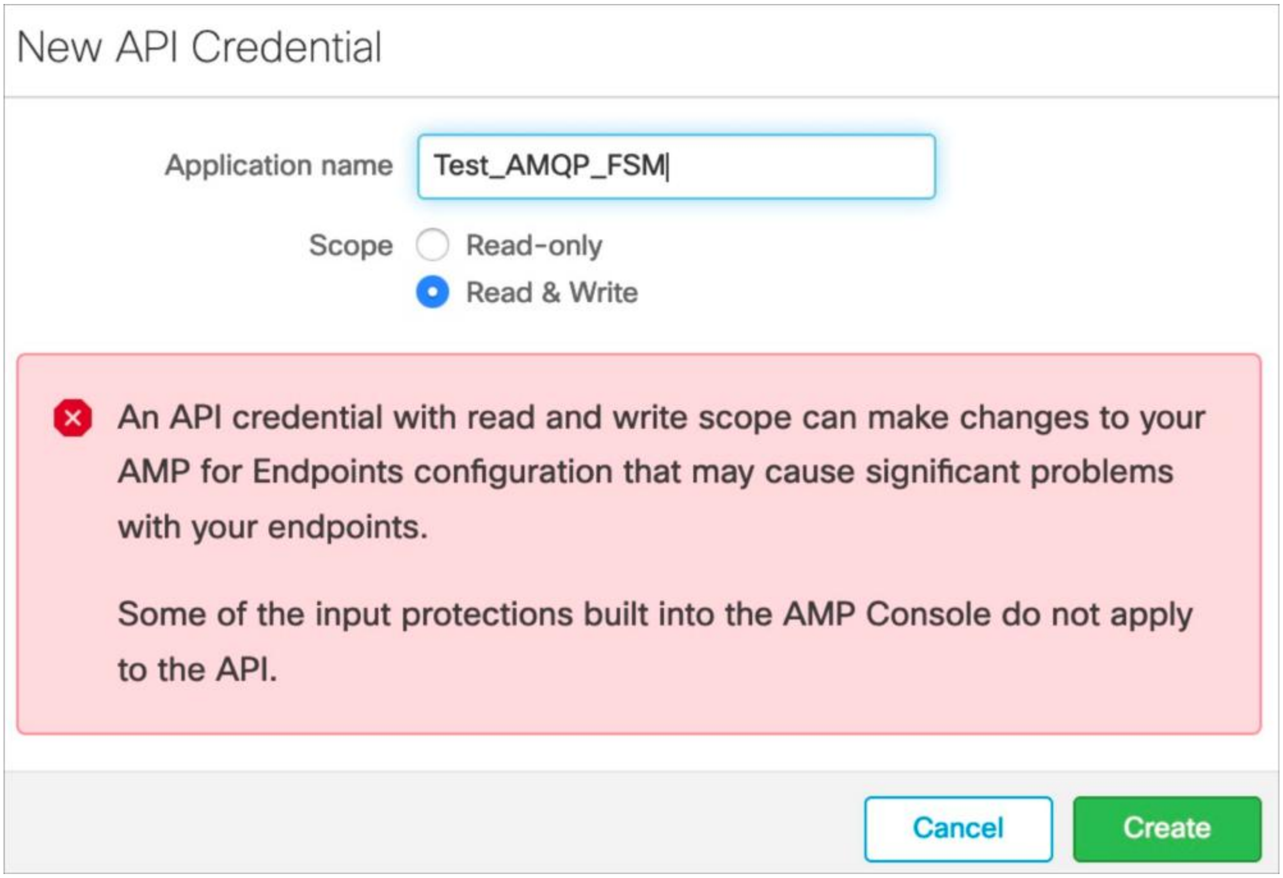
1. Log in to the Cisco AMP for Endpoints Portal as an administrator.
2. Click **Accounts > API Credentials**.



New AMP for Endpoints Mac Connector

Version 1.12.6.758 is now available. Learn more in the

3. In the API Credentials pane, click **New API Credential**.
4. In the **Application name** field, enter a name, and then select **Read & Write**.
   Note: you must have Read & Write access to manage event streams on your Cisco AMP for Endpoints platform.



New API Credential

Application name: Test_AMQP_FSM

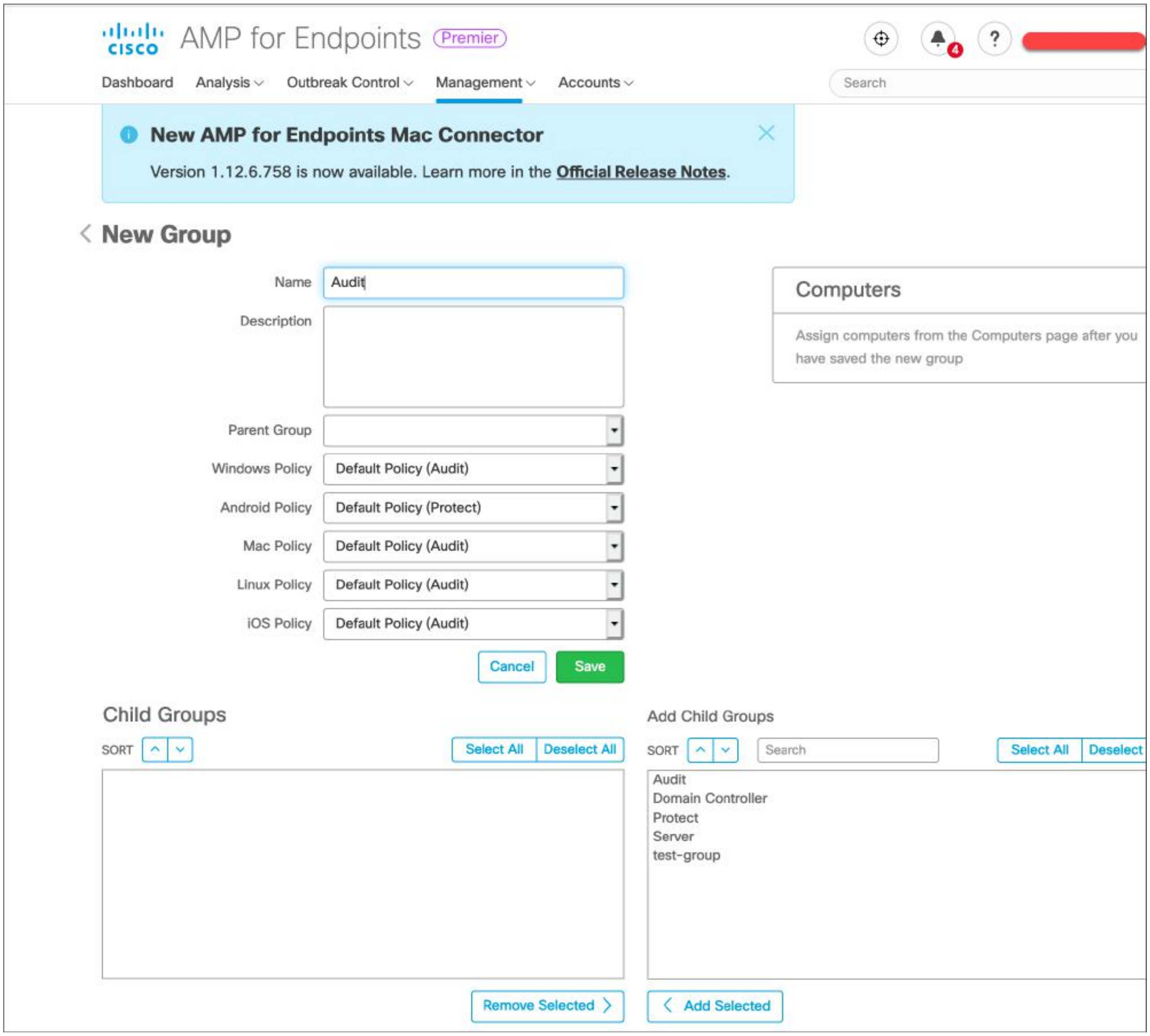
Scope ○ Read-only
● Read & Write

An API credential with read and write scope can make changes to your AMP for Endpoints configuration that may cause significant problems with your endpoints.

Some of the input protections built into the AMP Console do not apply to the API.

5. Click **Create**.
6. In the **API Key Details** section, make note of the values for the **3rd Party API Client ID** and the **API Key.** You will need these values to manage queues.
7. Click **Management > Group**.
8. In the Groups pane, click **Create Group**.

9. Enter the group name and click **Save**.



[redacted]

New AMP for Endpoints Mac Connector

Version 1.12.6.758 is now available. Learn more in the **Official Release Notes**.

New Group

Name: Audit

Description:

Parent Group:

Windows Policy: Default Policy (Audit)

Android Policy: Default Policy (Protect)

Mac Policy: Default Policy (Audit)

Linux Policy: Default Policy (Audit)

iOS Policy: Default Policy (Audit)

Computers

Assign computers from the Computers page after you have saved the new group

Child Groups

Add Child Groups

Audit
Domain Controller
Protect
Server
test-group

10. Enter the following `curl` command to get the `group_guid` of the group that is created in the previous step.

```
curl -X GET -H 'accept: application/json' \
   -H 'content-type: application/json' --compressed \
   -H 'Accept-Encoding: gzip, deflate' \
   -u <CLIENTID:APIKEY>\
   'https://api.amp.cisco.com/v1/groups'
```

where:

- `<CLIENTID:APIKEY>` is the Client ID and the API key that you created in Step 6.
- If you are in the Asia Pacific Japan and China (APJC) region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.apjc.amp.cisco.com/v1/event_streams`.
- If you are in the European region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.eu.amp.cisco.com/v1/event_streams`.

11. Enter the following `curl` command to create a Cisco AMP event stream:

```
curl -X POST -H 'accept: application/json' \
   -H 'content-type: application/json' --compressed \
   -H 'Accept-Encoding: gzip, deflate' \
   -d '{"name":"<STREAM_NAME>"}' \
   -u <CLIENTID:APIKEY> \
   'https://api.amp.cisco.com/v1/event_streams'
```

where:

- `<STREAM_NAME>` is the name of your choice for the event stream.
- `<CLIENTID:APIKEY>` is the Client ID and the API key that you created in Step 6.
- If you are in the Asia Pacific Japan and China (APJC) region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.apjc.amp.cisco.com/v1/event_streams`.
- If you are in the European region, change `https://api.amp.cisco.com/v1/event_streams` to `https://api.eu.amp.cisco.com/v1/event_streams`.
  Note: Only the event stream name is required. In the absence of `event_type` or `group_guid`, the stream will collect events from all groups and all event types.

12. Enter the following `curl` command to get a summary of the information you need to get a CloudAMP V1 credential in FortiSIEM:

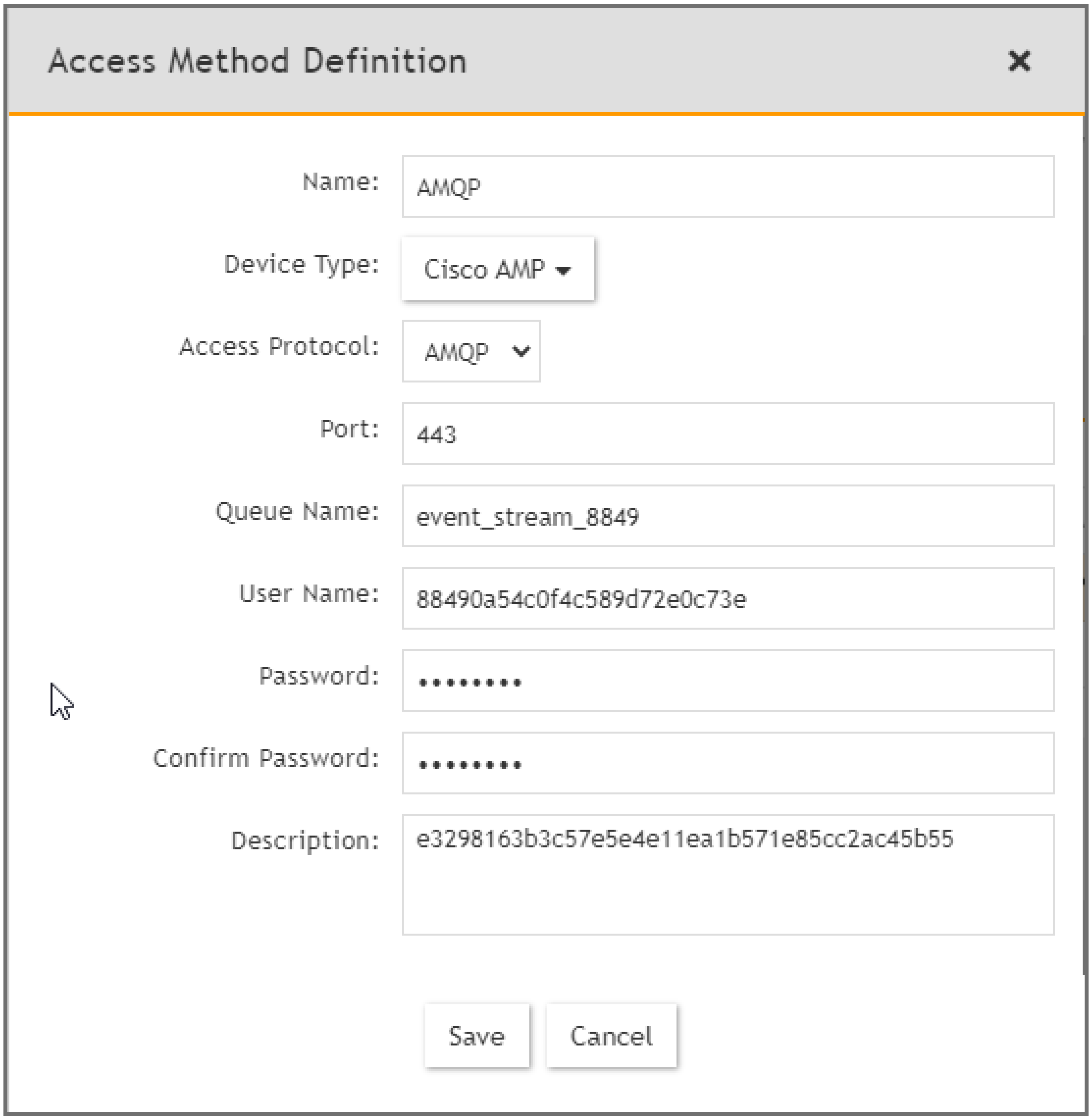
```
curl -X POST -H 'accept: application/json' \
   -H 'content-type: application/json' --compressed \
   -H 'Accept-Encoding: gzip, deflate' \
   -d '{"name":"meistream","group_guid":["34e483f4-85a8-412f-9997-07dd3f0c29ea"]}' \
   -u a54c0f4c589d72e0c73e:14713974-eb93-420b-ad76-6e13943f87d4 \
   'https://api.amp.cisco.com/v1/event_streams'
   {
      "version": "v1.2.0",
      "metadata": {
      "links": {
      "self": "https://api.amp.cisco.com/v1/event_streams"
      }
   },
      "data": {
      "id": 8849,
      "name": "meistream",
      "group_guids": [
      "34e483f4-85a8-412f-9997-07dd3f0c29ea"
      ],
      "amqp_credentials": {
      "user_name": "8849-a54c0f4c589d72e0c73e",
      "queue_name": "event_stream_8849",
      "password": "e3298163b3c57e5e4e11ea1b571e85cc2ac45b55",
      "host": "export-streaming.amp.cisco.com",
      "port": "443",
      "proto": "https"
      }
   }
}
```

Define Cisco CloudAMP Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New**.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
1. b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential, for example, "AMQP".
Device Type	Cisco AMP
Access Protocol	AMQP
Queue Name	Use the `queue-name` in Step 12 of the previous section.
User Name	Use the `user_name` in Step 12 of the previous section.
Password	Use the `password` in Step 12 of the previous section.
Description	Description of the device.



Access Method Definition

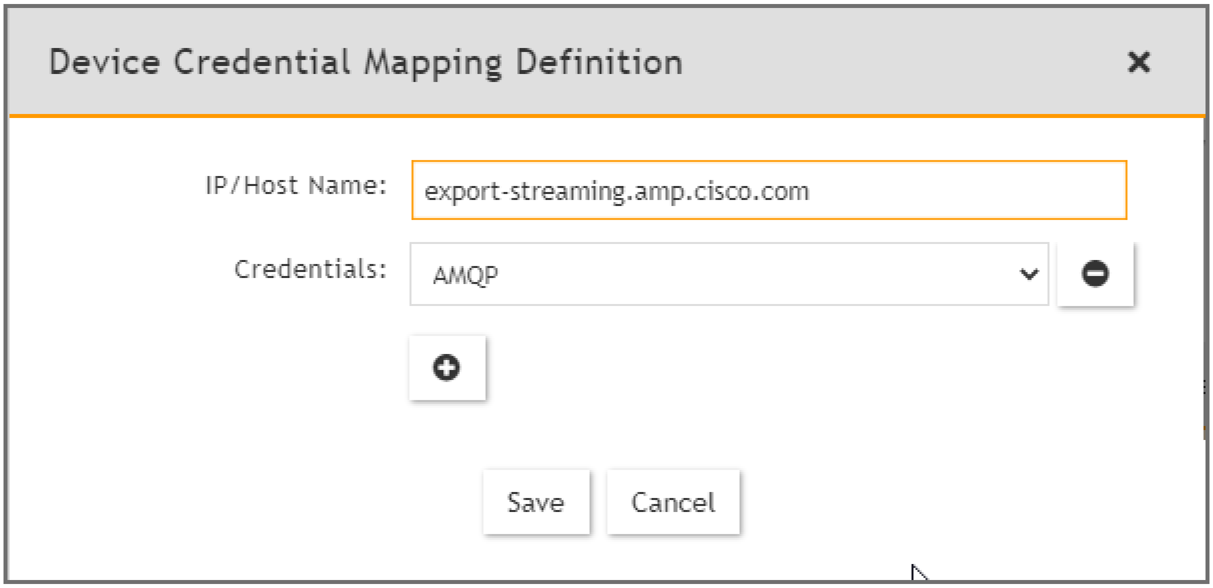
Name:	AMQP
Device Type:	Cisco AMP
Access Protocol:	AMQP
Port:	443
Queue Name:	event_stream_8849
User Name:	88490a54c0f4c589d72e0c73e
Password:	••••••••
Confirm Password:	••••••••
Description:	e3298163b3c57e5e4e11ea1b571e85cc2ac45b55

Create IP Range to Credential Association, Test Connectivity, and Event Pulling Check

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create your mapping.
   a. Enter the host in Step 12 of previous section into the **IP/Host Name** field.
   b. Select the name of the credential created in Define Cisco CloudAMP Credential in FortiSIEM from the **Credentials** drop-down list.

c. Click **Save**.



Device Credential Mapping Definition

IP/Host Name: export-streaming.amp.cisco.com

Credentials: AMQP

2. Select the entry just created, click the **Test** drop-down list, and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. If connectivity is successful, go to **ADMIN > Setup > Pull Events**. An entry will appear in the **Event Pulling** table. That means events are being pulled.

Sample Events

Events are in JSON format.

```
[CiscoAMP-Update-Policy-Failure]
{"id":6723137944535695384,"timestamp":1565352535,"timestamp_
nanoseconds":82000000,"date":"2019-08-09T12:08:55+00:00","event_type":"Policy Update
Failure","event_type_id":2164260866,"connector_guid":"98be064e-2ba5-4482-8405-
4a9268ae9f2e","group_guids":["3c025f05-a2c4-4613-9186-343365f53853"],"error":{"error_
code":3242196993,"description":"Unknown Error"},"computer":{"connector_guid":"98be064e-
2ba5-4482-8405-4a9268ae9f2e","hostname":"host1","external_
ip":"1.2.3.4","active":true,"network_addresses":
[{"ip":"1.2.3.5","mac":"00:21:97:1e:1c:05"}],"links":
{"computer":"https://api.amp.cisco.com/v1/computers/98be064e-2ba5-4482-8405-
4a9268ae9f2e","trajectory":"https://api.amp.cisco.com/v1/computers/98be064e-2ba5-4482-
8405-4a9268ae9f2e/trajectory","group":"https://api.amp.cisco.com/v1/groups/3c025f05-
a2c4-4613-9186-343365f53853"}}}
```

Cisco Security Agent (CSA)

- What is Discovered and Monitored
- Rules
- Reports
- Configuration
- Example SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Rules

FortiSIEM uses these rules to monitor events for this device:

Rule	Description
Agent service control	Attempts to modify agent configuration
Agent UI control	Attempts to modify agent UI default settings, security settings, configuration, contact information
Application control	Attempts to invoke processes in certain application classes
Buffer overflow attacks	
Clipboard access control	Attempts to acccess clipboard data written by sensitive data applications
COM component access control	Unusual attempts to access certain COM sets including Email objects
Connection rate limit	Excessive connections to web servers or from email clients
Data access control	Unusual attempts to access restricted data sets such as configuration files, password etc. by suspect applications
File access control	Unusual attempts to read or write restricted files sets such as system executables, boot files etc. by suspect applications

Rule	Description
Kernel protection	Unusual attempts to modify kernel functionality by suspect applications
Network access control	Attempts to connect to local network services
Network interface control	Attempts by local applications to open a stream connection to the NIC driver
Network shield	Attacks based on bad IP/TCP/UDP/ICMP headers, port and host scans etc
Windows event log	
Registry access control	Attempts to write certain registry entries
Resource access control	Symbolic link protection
Rootkit/kernel protection	Unusual attempts to load files after boot
Service restart	Service restarts
Sniffer and protocol detection	Attempts by packet/protocol sniffer to receive packets
Syslog control	Syslog events
System API control	Attempts to access Windows Security Access Manager (SAM)

Reports

There are no predefined reports for Cisco Security Agent.

Configuration

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example SNMP Trap

```
2008-05-13 11:00:36 192.168.1.39 [192.168.1.39]:SNMPv2-MIB::sysUpTime.0 = Timeticks:
      (52695748) 6 days, 2:22:37.48 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
      SMI::enterprises.8590.3.1 SNMPv2-SMI::enterprises.8590.2.1 = INTEGER: 619 SNMPv2-
      SMI::enterprises.8590.2.2 = INTEGER: 261 SNMPv2-SMI::enterprises.8590.2.3 = STRING:
      "sjdevVwindb06.ProspectHills.net"SNMPv2-SMI::enterprises.8590.2.4 = STRING: "2008-05-
      13 19:03:21.157" SNMPv2-SMI::enterprises.8590.2.5 = INTEGER: 5 SNMPv2-
```

```
SMI::enterprises.8590.2.6 = INTEGER: 452 SNMPv2-SMI::enterprises.8590.2.7 = STRING:
"C:\\Program Files\\RealVNC\\VNC4\\winvnc4.exe"SNMPv2-SMI::enterprises.8590.2.8 = NULL
 SNMPv2-SMI::enterprises.8590.2.9 = STRING: "192.168.20.38"SNMPv2-
SMI::enterprises.8590.2.10 = STRING: "192.168.1.39"SNMPv2-SMI::enterprises.8590.2.11 =
STRING: "The process 'C:\\Program Files\\RealVNC\\VNC4\\winvnc4.exe' (as user NT
AUTHORITY\\SYSTEM) attempted to accept a connection as a server on TCP port 5900 from
192.168.20.38 using interface Wired\\VMware Accelerated AMD PCNet Adapter. The
operation was denied." SNMPv2-SMI::enterprises.8590.2.12 = INTEGER: 109 SNMPv2-
SMI::enterprises.8590.2.13 = STRING: "192.168.1.39" SNMPv2-SMI::enterprises.8590.2.14
= STRING: "W"SNMPv2-SMI::enterprises.8590.2.15 = INTEGER: 3959 SNMPv2-
SMI::enterprises.8590.2.16 = INTEGER: 5900 SNMPv2-SMI::enterprises.8590.2.17 = STRING:
"Network access control"SNMPv2-SMI::enterprises.8590.2.18 = STRING: "Non CSA
applications, server for TCP or UDP services"SNMPv2-SMI::enterprises.8590.2.19 =
INTEGER: 33 SNMPv2-SMI::enterprises.8590.2.20 = STRING: "CSA MC Security
Module"SNMPv2-SMI::enterprises.8590.2.21 = NULL SNMPv2-SMI::enterprises.8590.2.22 =
STRING: "NT AUTHORITY\\SYSTEM"SNMPv2-SMI::enterprises.8590.2.23 = INTEGER: 2
```

CloudPassage Halo

- Integration Points
- CloudPassage REST API Integration
- Event Types
- Configuration

Integration Points

Protocol	Information collected	Used For
CloudPassage REST API	Halo– over 110 event types including User login and account activity, server compliance and vulnerability status, server FIM and firewall policy modification etc.	Security and Compliance

CloudPassage REST API Integration

FortiSIEM can pull logs from CloudPassage Halo via the CloudPassage REST API. Currently, over 110 CloudPassage event types are parsed.

Use cases covered via API:

- User login to Halo and user account creation/deletion/modification activity
- Vulnerable software package found and Compromised host detection
- Server FIM, Firewall policy modification
- Server account creation
- Server login via ghostport

Event Types

In **RESOURCES > Event Types**, search for "CloudPassage-Halo" in the main content panel **Search...** field to see the various event types for CloudPassage Halo.

Configuration

Take the following steps to configure CloudPassage Halo for FortiSIEM.

- Configuring CloudPassage Portal
- Define CloudPassage Halo Credential in FortiSIEM
- Create IP Range to Credential Association, Test Connectivity, and Event Checking

Configuring CloudPassage Portal

Create an API Key to be used for FortiSIEM communication.

1. Log in to your CloudPassage Halo portal.
2. Create an API Key and API Secret for use in FortiSIEM.

Define CloudPassage Halo Credential in FortiSIEM

Use the API Key and Secret in the previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	CloudPassage Halo
Access Protocol	Halo REST API
Pull Interval	5 minutes
Password config	For **CyberArk** and **RAX_CustomerService**, see Password Configuration. For **Manual**, see the following: 1. Set **API Key ID** to API Key obtained from the CloudPassage portal in Configuring CloudPassage Portal. 2. Set **API Key Secret** to API Secret obtained from the CloudPassage portal in Configuring CloudPassage Portal.
Organization	Choose the organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association, Test Connectivity, and Event Checking

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter "api.cloudpassage.com" in the **IP/Host Name** field.
   b. Select the name of the credential created in Define CloudPassage Halo Credential in FortiSIEM from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. Go to **ADMIN > Setup > Pull Events**. FortiSIEM will start to pull events from CloudPassage portal using the API.

4. Test for received CloudPassage Halo events by navigating to **ADMIN > Setup > Pull Events**, selecting a CloudPassage Halo event and clicking **Report**. The system will take you to the **ANALYTICS** tab and run a query to display the events received from CloudPassage in the last 15 minutes. You can modify the time interval to get more events.

CrowdStrike Endpoint Security

- Integration Points
- Falcon Streaming API Integration
- Falcon Data Replicator Integration

Integration Points

Protocol	Information Discovered	Used For
Falcon Streaming API	Detection Summary, Authentication Log, Detection Status Update, Indicators of Compromise, Containment Audit Events, IP White-listing events, Sensor Grouping Events.	Security and Compliance
Falcon Data Replicator	Detection Summary, User Activity, Authentication Activity.	Security and Compliance

Falcon Streaming API Integration

FortiSIEM can collect following types of events from CrowdStrike Cloud Service via Falcon Streaming API:

- Detection Summary
- Authentication Log
- Detection Status Update
- Customer Indicators of Compromise
- Containment Audit Events
- IP White-listing Events
- Sensor Grouping Events

CrowdStrike provides details about Falcon Streaming API here.

To receive Crowdstrike security events via Falcon Streaming API, follow these two steps:

1. Configure Crowdstrike Service for Falcon Streaming API
2. Configure FortiSIEM for Falcon Streaming API Based Access

Configure CrowdStrike Service for Falcon Streaming API

Create an account to be used for FortiSIEM communication:

1. Login to CrowdStrike as Falcon Customer Admin.
2. Go to **Support App** > **Key page**.
3. Click **Reset API Key**. Copy the API key and UUID for safe keeping. Note that your API key and UUID are assigned one pair per customer account, not one pair per user. Thus, if you generate a new API key, you may be affecting existing applications in your environment.

Configure FortiSIEM for Falcon Streaming API Based Access

Use the account in the previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a CrowdStrike Falcon Credential:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:
   c.

Settings	Description
Name	Enter a name for the credential
Device Type	CrowdStrike Falcon
Access Protocol	Falcon Streaming API
UUID	Enter the **UUID** for the credential created while Configuring CrowdStrike Service for Falcon Streaming API.
API Secret Key	Enter the **API Key Secret** for the credential created while Configuring CrowdStrike Service for Falcon Streaming API.
Organization	Choose the organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter "firehose.crowdstrike.com" in the **IP/Host Name** field.
   b. Select the name of the credential created in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results. Proceed to step 5 when connectivity succeeds.
5. An entry is created in **ADMIN > Setup > Pull Events** corresponding to the event pull job. FortiSIEM will start to pull events from the CrowdStrike Cloud service using the Falcon Streaming API.

To test for events received via CrowdStrike Streaming API:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the CrowdStrike Streaming API entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from CrowdStrike Cloud Service in the last 15 minutes. You can modify the time interval to get more events.

Falcon Data Replicator Integration

FortiSIEM can collect following types of events from CrowdStrike Cloud Service via Falcon Data Replicator method:

- Detection Summary Events
- User Activity Audit Events
- Auth Activity Audit Events

CrowdStrike provides details about Data Replicator method here.

To receive Crowdstrike security events via Falcon Data Replication Integration, follow these two steps:

1. Obtain AWS Credentials from Crowdstrike
2. Configure FortiSIEM for Falcon Data Replicator

Obtain AWS Credentials from CrowdStrike

Contact CrowdStrike to obtain AWS credentials for pulling CrowdStrike logs from AWS.

1. Generate a GPG key pair in ASCII format.
2. Send the public part of the GPG key to support@crowdstrike.com.
3. CrowdStrike will encrypt the API key with your public key and send you the encrypted API key. You can decrypt using your private GPG key.
4. CrowdStrike Support will also provide you an SQS Queue URL.

Credentials obtained in steps 3 and 4 above will be used in the next step.

Configure FortiSIEM for Falcon Data Replicator

Use the credentials in the previous step to enable FortiSIEM access. Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a CrowdStrike Data Replicator Credential:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:
   c.

Settings	Description
Name	Enter a name for the credential
Device Type	CrowdStrike Falcon
Access Protocol	CrowdStrike Falcon Data Replicator
Region	Enter the **Region** where the instance is located.
SQS Queue URL	Enter **SQS Queue URL** from here.
Password config	See Password Configuration.
Organization	Choose the organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Get the Hostname from the SQL Queue URL. For example, for Queue URL: `https://us-west-1.queue.amazonaws.com/754656674199/cs-prod-cannon-queue-`

`d5836cd3792ece8f`
set host name to `us-west-1.queue.amazonaws.com`.

   b. Select the name of the credential created in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results. Proceed to step 5 when connectivity succeeds.
5. An entry is created in **ADMIN > Setup > Pull Events** corresponding to the event pull job. FortiSIEM will start to pull events from the CrowdStrike Cloud service using the Falcon Streaming API.

To test for events received via CrowdStrike Falcon Data Replicator:

1. Go to **ADMIN** > **Setup** > **Pull Events**.
2. Select the CrowdStrike Falcon Data Replicator entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from CrowdStrike Cloud Service in the last 15 minutes. You can modify the time interval to get more events.

Digital Guardian Code Green DLP

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Event

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	1 event type	Security and Compliance

Event Types

In **RESOURCES > Event Types**, Search for "CodeGreen-" in the main content panel **Search...** field to see event types.

Rules

There are no specific rules, but generic rules for Data Leak Protection apply.

Reports

There are no specific reports, but generic rules for Data Leak Protection and Generic Servers apply.

Configuration

Configure Digital Guardian Code Green DLP to send syslog on port 514 to FortiSIEM.

Sample Event

```
<10>1 2017-05-11T12:08:06.380Z ABC-Manager DLP - INCADD incident_id="1.12815.1" managed_
device_id="1" number_of_incidents="1" incident_status="New,Audit Only" matched_policies_by_
severity="High:C_PHI_MRN / C_MRN_>25;" action_taken="NET_NS_H" matches="55" protocol="SMTP"
http_url="" inspected_document="Milla_9.16-4.17__UPDATED.XLSX" source="abc@cda.org" source_
ip="1.1.1.1" source_port="21752" destination="abc@bcd.edu" destination_ip="2.2.2.2"
destination_port="25" email_subject="RE: Open Encounters" email_sender="abc@cde.org" email_
recipients="abc@bcd.edu;" timestamp="2017-05-11 12:06:09 PDT" incidents_
url=https://aaa.lpch.net/LoadIncidentManagement.do?m=1&id=1,27372
```

ESET NOD32 Anti-Virus

- What is Discovered and Monitored
- ESET NOD32 Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

ESET NOD32 Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslog should be sent, enter the IP address of your FortiSIEM Supervisor.
- For **Port**, enter **514**.
- The syslog format should be the same as that shown in the example.

Example Syslog

```
<35313912>Jul 26 18:06:12 HOST01 ERA Server: [2011-07-26 13:06:12.784] V5 [4e2f02148110]
[00000e9c] <SESSION_INFO> Kernel connection from 10.0.52.25:48071 accepted

<35313864>Jul 26 18:06:13 HOST01 ERA Server: [2011-07-26 13:06:13.221] V5 [4e2f02148110]
[00000e9c] <SESSION_INFO> Kernel connection from
10.0.52.25:48071 closed (code 0,took 438ms, name 'HostExample01', mac '00-1E-4F-E8-49-03',
product 'ESET NOD32 Antivirus BUSINESS EDITION',
product version '04.00002.00071', virus signature db version '63(20110726)')
```

FortiClient

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Access Credentials for FortiSIEM
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog via FortiAnalyzer (FortiClient > FortiAnalyzer -> FortiSIEM)		Traffic logs (IPSec, VPN, File Cleaning/Blocking) Event logs (Antivirus, Web Filter, Vulnerability Scan, Application Firewall, VPN, WAN Optimization, Update logs)	Security Monitoring and Log analysis

Note: FortiSIEM collects logs from FortiAnalyzer (FAZ).

Event Types

Search for "FortiClient" in the main content panel **Search...** field to see the event types associated with this device under **RESOURCES** > **Event Types**.

Rules

There are generic rules that trigger for this device as event types are mapped to specific event type groups.

Reports

Generic reports are written for this device as event types are mapped to specific event type groups.

Configuration

Configuring FortiClient to send events to FortiAnalyzer (FAZ).

1. Configure FortiClient to send events to FAZ by following the steps in the knowledge base article How to integrate EMS in the FortiAnalyzer.

2. Configure FAZ to send events to FortiSIEM:
   a. Login to FAZ.
   b. Go to **System Settings** > **Advanced** > **Syslog Server**.
   c. Click **Create New**.
   d. Enter the **Name**. It is recommended to use the name of the FortiSIEM Supervisor node.
   e. Set the **IP address (or FQDN)** field to the IP or a fully qualified name of the FortiSIEM node that would parse the log (most likely Collector or Worker/Supervisor).
   f. Retain the **Syslog Server Port** default value '514'.
   g. Click **OK** to save your entries.
   h. Go to **System Settings** > **Dashboard** > **CLI Console**.
   i. Type the following in the CLI Console for:
      - FAZ 5.1 and older:

```
config system aggregation-client
   edit 1 (or the number for your FSM syslog entry)
   set fwd-log-source-ip original_ip
end
```

      - FAZ 5.6 and newer:

```
config system log-forward
  edit 1 (or the number for your FSM syslog entry)
  set fwd-log-source-ip original_ip
end
```

   j. Go to **System Settings** > **Log Forwarding**.
   k. Click **Create New**.
   l. Enter the **Name**.
   m. Select 'Syslog' as **Remote Server Type**.
   n. Enter the **Server IP** with the IP of the FortiSIEM Server/Collector.
   o. Retain the **Server Port** default value '514'.
   p. Set **Reliable Connection** to the default value 'Off'.
      Note: Setting this to 'On' will make every log sent from FAZ appear with FAZ's IP and NOT that of the firewall (s). In addition, your network must allow UDP connection between FAZ and FortiSIEM Collector. Otherwise, the logs will not reach the Collector.
   q. Optional – Use **Log Forwarding Filters** to select specific devices you want to forward log for.
3. Follow the steps below to validate that logs are properly flowing from FAZ to FortiSIEM:
   a. Login to FortiSIEM.
   b. Click **ANALYTICS** tab and use the filter to perform a real-time search:
      i. Click on the **Attribute** field to select 'Reporting IP' from the list or enter the same in the field to search.
      ii. Select '=' **Operator**.
      iii. In the **Value** field, enter the name of the Fortinet devices from where logs are expected.
      Note: This is NOT the IP address of the FAZ but of an original source device, like a FortiGate Firewall. To ensure that everything is being sent/received correctly, you can use multiple IPs.

   You will now see events from one, to numerous, source device(s), even though they are all forwarded from a single FAZ device. You can also check **CMDB** > **Devices** to see whether the devices are appearing within CMDB.

   Note: The Relaying IP value in FortiSIEM will not show the IP address of the FAZ but that of the original device which sent the logs to FAZ.

   All the device logs appear within FortiSIEM without configuring numerous devices individually.

Access Credentials for FortiSIEM

Setting	Value
Name	<name>
Device Type	Fortinet FortiClient
Access Protocol	WMI
Pull Interval	1 minute
NetBIOS/Domain	The NetBIOS name of servers or domain name
Password config	See Password Configuration

Sample Events

- Traffic Log
- Event Log

Traffic Log

```
<116> device=FCTEMS0000000001 severity=medium from=FAZVM64(FAZ-VM0000000001)
trigger=EVT2SIEM log="itime=1489562233 date=2017-03-15 time=00:17:13 logver=2
type=traffic sessionid=N/A hostname=hostname.local uid=1000000000
devid=FCT8000000000008 fgtserial=FCTEMS0000000005 level=warning regip=10.1.1.1
srcname="Opera" srcproduct=N/A srcip=10.1.1.3 srcport=18398 direction=outbound
dstip=10.0.0.4 remotename="aa.com" dstport=20480 user="bb.lee" service=http proto=6
rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=webfilter threat="Gambling"
vd=root fctver=1.2.1.1 os="Mac OS X 1.1.1" usingpolicy=N/A url=/ userinitiated=0
browsetime=N/A" ET---> FortiClient-traffic-blocked
```

Event Log

```
<116> device=FCTEMS0036759495 severity=medium from=FAZVM64(FAZ-VM0000000001)
trigger=EVT2SIEM1 log="itime=1490237155 date=2017-03-22 time=19:45:55 logver=2
level=info uid=C4C4E56CE7B04762B053E8F88B8ECF47 vd=root fctver=5.4.2.0862 os="Microsoft
Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)" usingpolicy=AOFCT
fgtserial=N/A emsserial=FCTEMS0036759495 devid=FCT8003883203338 hostname=sjcitvwfct01
pcdomain=accelops.net clientfeature=endpoint deviceip=devicemac=N/A type=event user=N/A
id=96953 msg="Endpoint Control Status changed - Offline""
```

Fortinet FortiEDR

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	System and Security Events (e.g., file blocked)	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, and search for "FortiEDR" to see the event types associated with this device.

Rules

No specific rules are written for FortiEDR but generic end point rules apply

Reports

No specific reports are written for FortiEDR but generic end point rules apply

Configuration

Configure FortiEDR system to send logs to FortiSIEM in the supported format (see Sample Events below)

Syslog Configuration

To configure syslog for FortiEDR, take the following steps:

Note: It is recommended you refer to the latest FortiEDR Administration Guide for the most current information. Steps provided here are based off the 5.0 FortiEDR Administration Guide (Refer to page 206).

1. Login to the FortiEDR Central Maanger.
2. Navigate to **Administration > Export Settings > Syslog**.

3. Click **Define New Syslog** and fill in the following fields.
   Note: If logs must pass across an unprotected medium, see the FortiEDR guide for Configuring Syslog over TLS on FortiSIEM collectors, and set port to 6514, protocol TCP, with Use SSL checked.

Field	Input
Name	Input "FortiSIEM".
Host	Enter the IP address or FQDN of the FortiSIEM Collector.
Port	Input "514".
Protocol	Select UDP.
Use SSL	Make sure the checkbox is unchecked.

4. Click the save icon to complete the configuration.

Configuration via API

Setup in FortiEDR

Take the following steps in FortiEDR.

1. Login to your FortiEDR device and to go **ADMINISTRATION > LICENSING > <*Name*>**.
2. Give REST API permission to a new or existing user in **ADMINISTRATION > USERS**.
3. Remember the user name and password for your setup in FortiSIEM.

Setup in FortiSIEM

FortiSIEM processes events from this via the Fortinet FortiEDR API. Configure and obtain the user name and password from the API before proceeding.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Fortinet FortiEDR
Access Protocol	FortiEDR_API
Pull Interval	5 minutes
Tenant ID	The FortiEDR tenant ID.
User Name	The user name for your FortiEDR account.
Password	The password for your FortiEDR account.

Settings	Description
Confirm Password	Input the same password as above for verification.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiEDR.
5. To see the jobs associated with FortiEDR, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "FortiEDR" in the search box.

Sample Events

```
<133>1 2019-09-18T06:42:18.000Z 1.1.1.1 enSilo - - - Organization: Demo;Organization ID: 156646;Event ID: 458478;
Raw Data ID: 1270886879;Device Name: WIN10-VICTIM;Operating System: Windows 10 Pro N;
Process Name: svchost.exe;Process Path: \Device\HarddiskVolume4\Windows\System32\svchost.exe;
Process Type: 64bit;Severity: Critical;Classification: Suspicious;Destination: File Creation;
First Seen: 18-Sep-2019, 02:42:18;Last Seen: 18-Sep-2019, 02:42:18;Action: Blocked;Count: 1;
Certificate: yes;Rules List: File Encryptor - Suspicious file modification;Users: WIN10-VICTIM\U;
MAC Address: 00-0C-29-D4-75-EC;Script: N/A;Script Path: N/A;Autonomous System: N/A;Country: N/A
```

Malwarebytes Breach Remediation

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Malware detection log	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "malwarebytesbreach" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 10 event types defined.

Rules

In **RESOURCES > Rules**, search for "Malware found but not remediated" in the main content panel **Search...** field.

Reports

In **RESOURCES > Reports**, search for "malware found" to see the reports associated with this device.

Examples include:

- Top Computers with Malware Found By Antivirus and Security Gateways
- Top IPs with Malware Found By Antivirus and Security Gateways
- Top IPs with Malware Found By Security Gateways

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
2020-11-25T17:18:46Z 0009NIT-KLUEY CEF:0|Malwarebytes|Malwarebytes Breach
Remediation|Version: 4.1.1.84 [eng:Version: 3.0.0.1090 rul:2020.11.25.17 act:Version:
3.2.0.266 sws:Version: 4.3.0.279]|1000|Scan Started|1|cs3=46837c42-2f42-11eb-9c15-
025041000001 cs3Label=SessionId cs5=mbbr  scan -full -remove -noreboot cs5Label=CmdLine
dvchost=0009NIT-KLUEY deviceMacAddress=DC:FB:48:92:E9:10 suser=TEST outcome=succeeded
```

Malwarebytes Endpoint Protection

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Malware detection log	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "malwarebytes-" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "Malware found but not remediated" in the main content panel **Search...** field.

Reports

In **RESOURCES > Reports**, search for "malware found" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<45>1 2016-09-23T14:40:35.82-06:00 reportDeviceName Malwarebytes-Endpoint-Security 1552 -
- {"security_log":{"client_id":"ef5f8fc8-ad0e-46f8-b6d7-1a85d5f73e64","host_name":"Abc-
cbd","domain":"abc.com","mac_address":"FF-FF-FF-FF-FF","ip_
address":"10.1.1.1","time":"2016-09-23T14:40:14","threat_level":"Moderate","object_
type":"FileSystem","object":"HKLM\\SOFTWARE\\POLICIES\\GOOGLE\\UPDATE","threat_
name":"PUM.Optional.DisableChromeUpdates","action":"Quarantine","operation":"QUARANTINE","
resolved":true,"logon_user":"dsamuels","data":"data","description":"No
description","source":"MBAM","payload":null,"payload_url":null,"payload_
process":null,"application_path":null,"application":null}}
```

McAfee ePolicy Orchestrator (ePO)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Traps			

Event Types

In **ADMIN > Device Support > Event Types**, search for "mcafee epolicy" to see the event types associated with this application or device.

Configuration

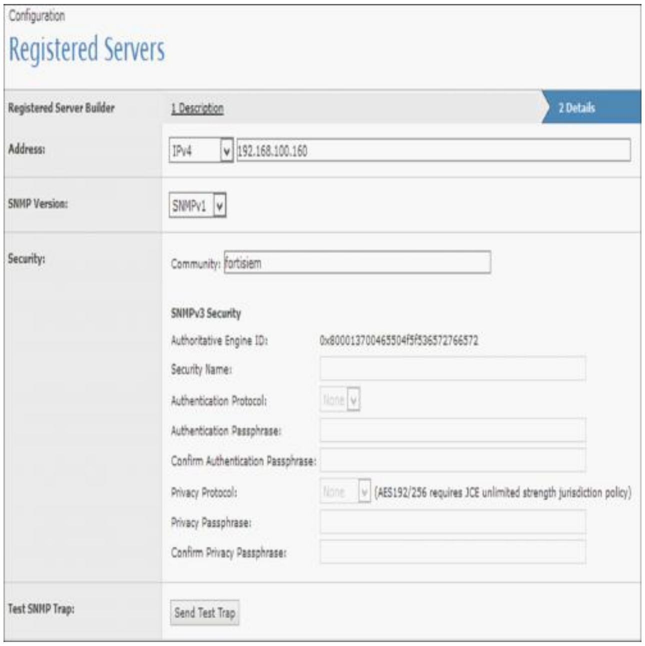
FortiSIEM processes events via SNMP traps sent by the device.

Follow the below procedures to configure McAfee ePO to send Threat based SNMP traps to FortiSIEM.

Step 1: Configuring SNMP Server to send Traps from McAfee ePO.

FortiSIEM processes events from a device via SNMP traps sent by the device.

1. Log in to the McAfee ePO web console.
2. Go to **Main Menu > Configuration > Registered Servers**, and click **New Server**.
   The **Registered Server Builder** opens.



Address: IPv4 192.168.100.160

SNMP Version: SNMPv1

Security:

Community: fortisiem

SNMPv3 Security

Authoritative Engine ID: 0x800013700465504f5f536572766572

Security Name:

Authentication Protocol: None

Authentication Passphrase:

Confirm Authentication Passphrase:

Privacy Protocol: None (AES192/256 requires JCE unlimited strength jurisdiction policy)

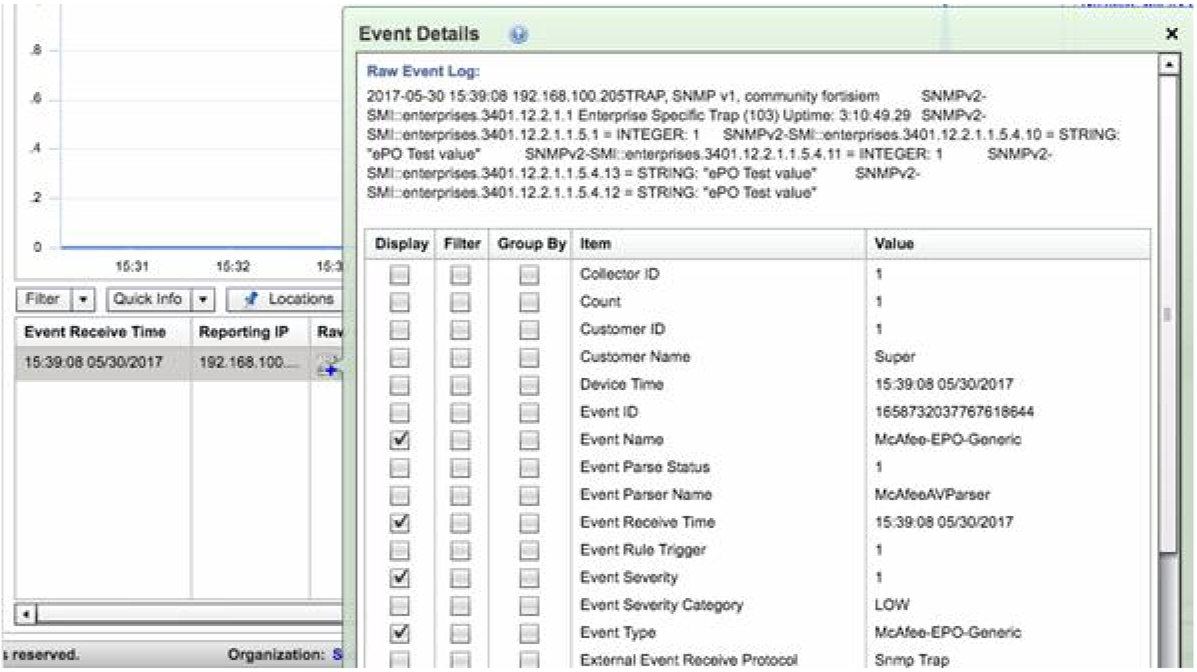
Privacy Passphrase:

Confirm Privacy Passphrase:

Test SNMP Trap:

3. For **Server type**, select **SNMP Server**.
4. For **Name**, enter the IP address of your SNMP server.
5. Enter any **Notes**, and click **Next** to go to the **Details** page.
6. For **Address**, select IP4 from the drop-down and enter the IP/DNS Name for the FortiSIEM virtual appliance and SNMP that will receive the SNMP trap.
7. For **SNMP Version**, select **SNMPv1**.
8. For **Community**, enter **public**.

   Note: The community string entered here would not be used in FortiSIEM as FortiSIEM accepts traps from McAfee ePO without any configuration.
9. Click **Send Test Trap**, and then click **Save**.
10. Log in to your Supervisor node and use Real Time Search to see if FortiSIEM received the trap. Without any configuration on FortiSIEM, the traps are received under Real time/Historical Analytics. (Search using 'Reporting IP' as McAfee ePO’s IP.)



Event Receive Time	Reporting IP	Rav
15:39:08 05/30/2017	192.168.100....	

Raw Event Log:

```
2017-05-30 15:39:08 192.168.100.205TRAP, SNMP v1, community fortisiem        SNMPv2-
SMI::enterprises.3401.12.2.1.1 Enterprise Specific Trap (103) Uptime: 3:10:49.29  SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.1 = INTEGER: 1     SNMPv2-SMI::enterprises.3401.12.2.1.1.5.4.10 = STRING:
"ePO Test value"        SNMPv2-SMI::enterprises.3401.12.2.1.1.5.4.11 = INTEGER: 1        SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.4.13 = STRING: "ePO Test value"        SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.4.12 = STRING: "ePO Test value"
```

Display	Filter	Group By	Item	Value
□	□	□	Collector ID	1
□	□	□	Count	1
□	□	□	Customer ID	1
□	□	□	Customer Name	Super
□	□	□	Device Time	15:39:08 05/30/2017
□	□	□	Event ID	1658732037767618644
☑	□	□	Event Name	McAfee-EPO-Generic
□	□	□	Event Parse Status	1
□	□	□	Event Parser Name	McAfeeAVParser
☑	□	□	Event Receive Time	15:39:08 05/30/2017
□	□	□	Event Rule Trigger	1
☑	□	□	Event Severity	1
□	□	□	Event Severity Category	LOW
☑	□	□	Event Type	McAfee-EPO-Generic
□	□	□	External Event Receive Protocol	Snmp Trap

Step 2: Configuring “Automatic Response”

By default, McAfee ePO does not send SNMP Trap alerts for the events that occur. This must be configured.

1. Go to **Main Menu** > **Automation** > **Automatic Response**.
2. By default, there are a few Automatic Response configured, but are in a disabled state.
3. Click on **New Response** button.
4. Enter a **Name** for the 'Response'.
5. Set **Status** as 'Enabled' and click **Next**.
6. Click the Ellipsis icon and select the top level under **Select System Tree Group** and click **OK**.
7. On the left side of the same screen, select Threat Handled.

Sample Access Protection Violation detected SNMP Trap

```
2017-05-30 16:24:27 192.168.100.205TRAP, SNMP v1, community fortisiem SNMPv2-
SMI::enterprises.3401.12.2.1.1 Enterprise Specific Trap (101) Uptime: 3:56:08.15
SNMPv2- SMI::enterprises.3401.12.2.1.1.5.7 = STRING: "Threat_Trigger_Rule"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.30 = STRING: "58F5DD64- 43C5-11E7-0584-000C29219964"
 SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.360 = STRING: "My Organization" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.20 = STRING: "05/30/17 13:20:24 UTC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.50 = STRING: "ENDP_AM_1050" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.510 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.510 = STRING: "Access Protection" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.520 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.70 = STRING: "WIN2012- SKULLC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.90 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.80 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.500 = STRING: "000c29219964" SNMPv2-
```

```
SMI::enterprises.3401.12.2.1.1.5.2.50 = STRING: "McAfee Endpoint Security"SNMPv2-
SMI::enterprises.3401.12.2.1.1.6.0.00 = STRING: "10.5.0" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.370 = STRING: "Access Protection rule violation
detected and NOT blocked" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.6 = STRING: "Threat"
SNMPv2-SMI::enterprises.3401.12.2.1.1.5.1 = INTEGER: 1 SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.390 = STRING: "Server" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.380 = STRING: "Windows Server 2012 R2" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.50 = STRING: "05/30/17 13:24:05 UTC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.530 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.550 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.540 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.560 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.580 = STRING: "FIREFOX.EXE" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.590 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.570 = STRING: "WIN2012-SKULLC\Administrator" SNMPv2-
 SMI::enterprises.3401.12.2.1.1.5.2.500 = STRING: "GlobalRoot\Directory\My
Group"SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.280 = STRING:
"C:\USERS\ADMINISTRATOR\DOWNLOADS\V3_2994DAT.EXE" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.200 = STRING: "WIN2012- SkullC" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.220 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.210 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.230 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.250 = STRING: "0" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.270 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.260 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.240 = STRING: "SYSTEM" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.340 = STRING: "IDS_ACTION_WOULD_BLOCK" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.290 = STRING: "'File' class or access"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.300 = STRING: "1095"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.350 = STRING: "True"SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.320 = STRING: "Browsers launching files from the
Downloaded Program Files folder"SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.310 =
STRING: "Critical" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.330 = STRING: "Access
Protection"
```

MobileIron Sentry and Connector

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Syslog	Host name and Device Type from LOG	Over 14 types of security logs	Security and Compliance

Event Types

Go to **ADMIN > Device Support > Event Types** and search for "MobileIron-".

Rules

None

Reports

None

Configuration

Configure MobileIron to send syslog in the supported format to FortiSIEM. No configuration is required in FortiSIEM.

Sample Events

```
Apr  3 04:16:51 mobile-apptunnel.xxxxx.com mi: PRODUCT=Sentry_9.4.0_4,2019 Apr  3 04:16:48
WARN   (Device=bc7b8d61-b003-49e6-9ef5-76ee5bebd6d9, DeviceIPPort=10.1.1.1:60995,
User=Username2, Command=POST, Server=25678:domain3.local, Service=Traveler)
(AlertOrigin=Sentry, AlertId=HTTP503) Got exception during device-to-server processing,
Sentry reporting error to client:java.net.SocketTimeoutException: Read timed out
```

Netwrix Auditor (via Correlog Windows Agent)

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Via Correlog Windows Agent	Host name and Device Type from LOG	2 Security logs	Security and Compliance monitoring

Event Types

Go to **ADMIN > Device Support > Event Types** and search for "Netwrix_Auditor_".

Rules

None

Reports

None

Configuration

Configure Netwrix Auditor to send logs to Correlog Windows Agent. FortiSIEM will automatically parse the logs as long as they appear in the format below.

Sample Events

```
<158>2018 Jul 27 07:20:36 CorreLog_Win_Agent ACME-NETWRIX Netwrix_Auditor_Integration 0:
Netwrix_Auditor_Integration_API: DataSource : Windows Server Action : Removed Message:
Removed DNS A Where : ACME-DC02 ObjectType : DNS A Who : system What : DNS Server\SAC-
DC02\acmegroup.local\ACME-TRADE08 IN A 10.150.90.180 1200 When : 2018-07-27T14:15:43Z
Details : IP Address: 10.150.90.180, TTL: 1200, Container name: acmegroup.local, Owner name:
acmegroup.local -
```

Palo Alto Traps Endpoint Security Manager

- What is Discovered and Monitored
- Event Types
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	Over 150 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "PAN-TrapsESM" in the main content panel **Search...** field.

Sample Event Type

```
Sep 28 2016 17:38:48 172.16.183.173 CEF:0|Palo Alto Networks|Traps Agent|3.4.1.16709|Traps
Service Status Change|Agent|6|rt=Sep 28 2016 17:38:48 dhost=traps-win7x86 duser=Traps
msg=Agent Service Status Changed: Stopped-> Running
```

```
Sep 28 2016 17:42:04 ESM CEF:0|Palo Alto Networks|Traps ESM|3.4.1.16709|Role
Edited|Config|3|rt=Sep 28 2016 17:42:04 shost=ESM suser=administrator msg=Role TechWriter
was added\changed
```

Configuration

Configure Palo Alto Traps Endpoint Security Manager to send syslog on port 514 to FortiSIEM.

SentinelOne

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

Integration Points

Method	Information Discovered	Metrics Collected	Logs Collected	Used for
Syslog	Host name, Reporting IP	None	System and Security Events (e.g., file blocked)	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "SentinelOne" to see the event types associated with this device.

Rules

No specific rules are written for SentinelOne but generic end point rules apply.

Reports

No specific reports are written for SentinelOne but generic end point rules apply.

Configuration

Configure SentinelOne system to send logs to FortiSIEM in the supported format (see Sample Events).

Settings for Access Credentials

None required.

Sample Events

```
<14>CEF:0|SentinelOne|Mgmt|Windows 7|21|Threat marked as resolved|1|rt=Jun 05 2017
09:29:17 uuid=586e7cc578207a3f75361073
fileHash=4b9c5fe8ead300a0be2dbdbcdbd193591451c8b4
filePath=\Device\HarddiskVolume2\Windows\AutoKMS\AutoKMS.exe
```

```
<14>CEF:0|SentinelOne|Mgmt|1.1.1.1|65|user initiated a fetch full report command to the
agent DT-Virus7|1|rt=#arcsightDate(Jun 06 2017 09:29:17) suser=xyz
duid=c29ca0cee8a0a989321495b78b1d256ab7189144 cat=SystemEvent
```

Sophos Central

- Integration Points
- Event Types
- Configuring Sophos Central for API Access
- Configuring FortiSIEM for Sophos Central for API Access

Integration Points

Protocol	Information Discovered	Used For
Sophos Central API	Endpoint suspicious activity detected by Sophos agent	Security and Compliance

Event Types

Over 20 events are parsed. See event types in **RESOURCES** > **Event Types** by searching for "Sophos-Central" in the main content panel **Search...** field.

Configuring Sophos Central for API Access

Sophos provides ample documentation here.

1. Login to Sophos Central Website.
2. Go to **Global Settings** > **API Token Management**. Click **Add Token**.
   The Token will display.
3. Note the following information for later use:
   a. Get **Host Name** from **API Access URL** (part after https://).
   b. Get **Authorization** from **API Access URL + Headers** (part after Authorization:Basic).
   c. Get **API Key** from Headers (part between **x-api-key**: and **Authorization Basic**).

Configuring FortiSIEM for Sophos Central for API Access

Use the account in the previous step to enable FortiSIEM access. For FortiSIEM configuration, follow the steps here.

- Define Sophos Central Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity
- Viewing Pull Events

Define Sophos Central Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a Sophos Central credential.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Sophos Central
Access Protocol	Sophos Central API
Authorization	Enter the **Authorization** created in the previous section - step 3b above.
URI	Leave the **URI** field empty. FortiSIEM will use `gateway/siem/v1/events`.
API Key	Enter the **API Key** created in the previous section - step 3c.
Organization	Choose the organization if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter the **Hostname** created here - step 3a in the **IP/Host Name** field.
   b. Select the name of the credential created in step 2 of Define Sophos Central Credential in FortiSIEM from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results. If it succeeds, the credential is correct.
3. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Sophos Central using the Sophos Central API.

Viewing Pull Events

To view events received via Windows Defender ATP REST API:

1. Go to **ADMIN** > **Setup** > **Pull Events**.
2. Select the Windows Defender ATP entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from Sophos Central in the last 15 minutes. You can modify the time interval to get more events.

Sophos Endpoint Security and Control

- What is Discovered and Monitored
- Event Types
- Sophos Configuration
- Sample SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Event Types

In **ADMIN > Device Support > Event Types**, search for "sophos endpoint" to see the event types associated with this application or device.

Sophos Configuration

SNMP Trap

FortiSIEM processes Sophos Endpoint control events via SNMP traps sent from the management console. Configure the management console to send SNMP traps to FortiSIEM, and the system will automatically recognize the messages.

SNMP Traps are configured within the Sophos policies.

1. In the **Policies** pane, double-click the policy you want to change.
2. In the **policy** dialog, in the **Configure** panel, click **Messaging**.
3. In the **Messaging** dialog, go to the **SNMP messaging** tab and select **Enable SNMP messaging**.
4. In the **Messages to send** panel, select the types of event for which you want Sophos Endpoint Security and Control to send SNMP messages.
5. In the **SNMP trap destination** field, enter the IP address of the recipient.
6. In the **SNMP community name** field, enter the SNMP community name.

Sample SNMP Trap

```
2011-05-03 18:22:32 172.15.30.8(via UDP: [172.15.30.8]:1216) TRAP, SNMP v1, community public
SNMPv2-SMI::enterprises.2604.2.1.1.1 Enterprise Specific Trap (1) Uptime: 5:59:55.31
SNMPv2-SMI::enterprises.2604.2.1.1.2.1.1 = STRING: "File
\"C:\WINDOWS\system32\LDPackage.dll\" belongs to virus/spyware 'Mal/Generic-S'."SNMPv2-
SMI::enterprises.2604.2.1.1.2.2.2 = STRING: "9.5.5"
```

Symantec Endpoint Protection

- What is Discovered and Monitored
- Event Types
- Symantec Endpoint Protection Configuration
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "symantec endpoint" to see the event types associated with this device.

Symantec Endpoint Protection Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device.

- Configuring Log Transmission to FortiSIEM
- Configuring the Types of Logs to Send to FortiSIEM

Configuring Log Transmission to FortiSIEM

1. Log in to Symantec Endpoint Protection Manager.
2. Go to **Admin> Configure External Logging > Servers > General**.
3. Select **Enable Transmission of Logs to a Syslog Server**.
4. For **Syslog Server**, enter the IP address of the FortiSIEM virtual appliance.
5. For **UDP Destination Port**, enter **514**.

Configuring the Types of Logs to Send to FortiSIEM

1. Go to **Admin> Configure External Logging > Servers > Log Filter**.
2. Select the types of logs and events you want to send to FortiSIEM.

Sample Syslog

```
<13>Feb 23 12:36:37 QA-V-Win03-App1.ProspectHills.net SymAntiVirus  0
2701170C2410,3,2,1,QA-V-WIN03-APP1,Administrator,,,,,,,16777216,"Scan started on selected
```

```
drives and folders and all extensions.",1235421384,,0,,,,,0,,,,,,,,,,,{C11B44CF-35C9-4342-
AB3D-E0E9E3756510},,(IP)-
0.0.0.0,,ACME,00:50:56:A3:30:2F,11.0.1000.1112,,,,,,,,,,,,,,,,0,,,,,
<54>Jun 11 12:24:38 SymantecServer sjdevswinapp05: Site: Site sjdevswinapp05,Server:
sjdevswinapp05,Domain: Default,Admin: admin,Administrator  log on failed
<54>Jun 11 12:24:51 SymantecServer sjdevswinapp05: Site: Site sjdevswinapp05,Server:
sjdevswinapp05,Domain: Default,Admin: admin,Administrator  log on succeeded
<54>Feb 23 13:08:29 SymantecServer sjdevswinapp05: Virus found,Computer name: Filer,Source:
Real Time Scan,Risk name: EICAR Test String,Occurrences: 1,C:/Documents and
Settings/Administrator.PROSPECTHILLS/Local Settings/Temp/vpqz3cxj.com,"",Actual action:
Cleaned by deletion,Requested action: Cleaned,Secondary action: Quarantined,Event time:
2009-02-23 21:06:51,Inserted: 2009-02-23 21:08:29,End: 2009-02-23 21:06:51,Domain:
Default,Group: Global\Prospecthills,Server: sjdevswinapp05,User: Administrator,Source
computer:  ,Source IP: 0.0.0.0

Mar 16 15:11:06 SymantecServer aschq97: NF77088-PCA,Local: 192.168.128.255,Local: 138,Local:
FFFFFFFFFFFF,Remote: 192.168.128.86,Remote: ,Remote: 138,Remote:
0015C53B9216,UDP,Inbound,Begin: 2009-03-16 15:05:02,End: 2009-03-16 15:05:02,Occurrences:
1,Application: C:/WINDOWS/system32/ntoskrnl.exe,Rule: Allow local file sharing,Location:
Default,User: ,Domain: ASC
<54>Feb 24 11:51:19 SymantecServer sjdevswinapp05: QA-V-Win03-App2,[SID: 20352] HTTP
Whisker/Libwhisker Scan (1) detected.  Traffic has been allowed from this application:
C:\WINDOWS\system32 toskrnl.exe,Local: 0.0.0.0,Local: 000000000000,Remote: ,Remote:
192.168.1.4,Remote: 000000000000,Inbound,TCP,Intrusion ID: 0,Begin: 2009-02-24 11:50:01,End:
2009-02-24 11:50:01,Occurrences: 1,Application: C:/WINDOWS/system32/ntoskrnl.exe,Location:
Default,User: Administrator,Domain: PROSPECTHILLS
<54>Jul 28 08:08:52 SymantecServer corpepp01: 6910p-X751008R,Category: 2,Symantec
AntiVirus,New virus definition file loaded. Version: 130727ag.
<54>Jul 28 08:09:32 SymantecServer corpepp01: CORPMIO-H4VYWB1,Category: 2,Symantec
AntiVirus,Symantec Endpoint Protection services shutdown was successful.
<52>Jul 28 08:10:13 SymantecServer corpepp01: TEMPEXP02,Category: 0,Smc,Failed to disable
Windows firewall
<54>Jul 28 08:08:52 SymantecServer corpepp01: 8440p-X0491JYR,Category: 0,Smc,Connected to
Symantec Endpoint Protection Manager (10.0.11.17)
<54>Jul 28 08:08:52 SymantecServer corpepp01: 8440p-X0491JYR,Category: 0,Smc,Disconnected
from Symantec Endpoint Protection Manager (10.0.11.17)
<54>Jul 28 08:09:52 SymantecServer corpepp01: CORPES-3042,Category: 0,Smc,Connected to
Symantec Endpoint Protection Manager (corphqepp01)
<54>Jul 28 08:09:52 SymantecServer corpepp01: CORPES-3042,Category: 0,Smc,Disconnected from
Symantec Endpoint Protection Manager (corpepp01)
<54>Jul 28 08:09:32 SymantecServer corpepp01: CORPMIO-H4VYWB1,Category: 0,Smc,Network Threat
Protection - - Engine version: 11.0.480  Windows Version info:  Operating System: Windows XP
(5.1.2600 Service Pack 3)  Network  info:  No.0  "Local Area Connection 3"  00-15-c5-46-58-
1e  "Broadcom NetXtreme 57xx Gigabit Controller" 10.0.208.66
<54>Jul 28 07:55:32 SymantecServer corpepp01: tol-afisk,Blocked,Unauthorized NT call
rejected by protection driver.,System,Begin: 2011-07-27 15:29:57,End: 2011-07-27
15:29:57,Rule: Built-in rule,6092,AcroRd32.exe,0,None,"FuncID=74H, RetAddr=18005CH",User:
afisk,Domain: HST
```

Symantec SEPM

- Configuring Symantec SEPM
- Receiving Events in FortiSIEM

Configuring Symantec SEPM

follow these steps to configure Symantec SEPM to send logs to FortiSIEM. For more information about Symantec SEPM, see the *SEPM Installation and Administration Guide*: https://support.symantec.com/us/en/article.DOC10654.html

1. In the Symantec SEPM console, go to **Admin > Servers**.
2. Click the local site or remote site that you want to export log data from.
3. Click **Configure External Logging**.
4. On the **General** tab, in the **Update Frequency** list box, select how often to send the log.
5. In the **Master Logging Server** list box, select the management server to send the logs to. If you use SQL Server and connect multiple management servers to the database, then specify only one server as the **Master Logging Server**.
6. Check **Enable Transmission of Logs to a Syslog Server** (FortiSIEM).
7. Provide the following information. Be sure that syslog server IP and Port can be reached from SEPM.
    a. **Syslog Server**—Enter the IP address or domain name of the Syslog server that will receive the log data (in this case, the IP of FortiSIEM).
    b. **Destination Port**—Select the protocol to use, and enter the destination port that the Syslog server uses to listen for Syslog messages. (for example, UDP 514 for FortiSIEM).
    c. **Log Facility**—Enter the number of the log facility that you want to the Syslog configuration file to use, or use the default value. Valid values range from 0 to 23.
8. On the **Log Filter** tab, check which logs to export

Receiving Events in FortiSIEM

1. Check for events in FortiSIEM. Go to the **ANALYTICS** page and search for "Symantec".
2. Check for the device added by log. Go to **CMDB > Devices**.

Tanium Connect

- Integration Points
- Event Types
- Configuring Tanium Connect
- Configuring FortiSIEM

Integration Points

Protocol	Information Discovered	Used For
Sophos Central API	Endpoint security logs	Security and Compliance

Event Types

Currently, 4 events are parsed. See event types in **RESOURCES** > **Event Types** and search for "TaniumConnect-" in the main content panel **Search...** field. The user can extend the parser to add other events.

Configuring Tanium Connect

Follow Tanium Connect documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes Tanium Connect syslog as long it follows the following format as shown in the sample syslog:

```
<134>1 2018-09-06T02:50:02.762000+00:00 tanium-server-1 Tanium 7020 - [Comply-
Deployment-Status---Deployment-5@017472 Installed=true Version=3.0.45 Type=full
Installed1=true Version1=8u131-e1 Comply---Has-Latest-Tools=true Count=2
```

Trend Micro Interscan Web Filter

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	15 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "TrendMicro-InterscanWeb-" in the main content panel **Search...** field.

Sample Event Type:

```
<130>abc.com: <Mon, 18 Sep 2017 10:00:48,IST> [EVT_URL_BLOCKING|LOG_CRIT] Blocked URL log
tk_username=1.1.1.1,tk_date_field=2017-09-18 10:00:48+0530,tk_protocol=https,tk_
url=https://google.com:443/,tk_malicious_entity=,tk_file_name=,tk_entity_name=,tk_
action=,tk_scan_type=user defined,tk_blocked_by=rule,tk_rule_name=google.com,tk_opp_id=0,tk_
group_name=None,tk_category=URL Blocking,tk_uid=0099253425-0ecd0076872a9d0ace16,tk_filter_
action=0
```

```
<134>abc.com: <Mon, 18 Sep 2017 10:00:48,IST> [EVT_URL_ACCESS_TRACKING|LOG_INFO] Access
tracking log tk_username=1.1.1.1,tk_url=http://aaa.com/pc/SHAREitSubscription.xml,tk_
size=0,tk_date_field=2017-09-18 10:00:48+0530,tk_protocol=http,tk_mime_
content=unknown/unknown,tk_server=abc.com,tk_client_ip=1.1.1.1,tk_server_ip=2.2.2.2,tk_
domain=aaa.com,tk_path=pc/SHAREitSubscription.xml,tk_file_name=SHAREitSubscription.xml,tk_
operation=GET,tk_uid=0099253421-bdd7d4ce063b924a2342,tk_category=56,tk_category_type=0
```

```
<134>abc.com: <Mon, 18 Sep 2017 10:00:59,IST> [EVT_PERFORMANCE|LOG_INFO] Performance log tk_
server=abc.com,tk_date_field=2017-09-18 10:00:59+0530,tk_metric_id=Number of FTP
Processes,tk_metric_value=6,
```

Rules

There are no specific rules, but generic rules for Web Filters and Generic Servers apply.

Reports

There are no specific reports, but generic rules for Web Filters and Generic Servers apply.

Configuration

Configure TrendMicro Interscan Web Filter to send syslog on port 514 to FortiSIEM.

Trend Micro Intrusion Defense Firewall (IDF)

- What is Discovered and Monitored
- Trend Micro Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Trend Micro Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog

```
<134>May 31 15:24:34 DSK-FT11XL1 dsa_mpld: REASON=PLD:Disallow_Web_Proxy_Autodiscovery_
Protocol REV IN= OUT=Local_Area_Connection
MAC=00:26:B9:80:74:71:2C:6B:F5:35:4E:00:08:00 SRC=192.168.20.2 DST=192.168.13.39 LEN=133
PROTO=UDP SPT=53 DPT=58187 CNT=1 act=Reset POS=0
SPOS=0 NOTE=CVE-2007-5355 FLAGS=0
```

Trend Micro OfficeScan

- What is Discovered and Monitored
- Configuration
- Example SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Configuration

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example SNMP Trap

```
2011-04-14 02:17:54 192.168.20.214(via UDP: [192.168.20.214]:45440) TRAP, SNMP v1, community
public    SNMPv2-SMI::enterprises.6101 Enterprise Specific Trap (5) Uptime: 0:00:00.30
SNMPv2-SMI::enterprises.6101.141 = STRING: "Virus/Malware: Eicar_test_file Computer:
SJDEVVWINDB05 Domain: ABC File: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\yc8eayj0.com Date/Time:
4/10/2008 14:23:26 Result: Virus successfully detected, cannot perform the Clean action
(Quarantine) "
```

Firewalls

FortiSIEM supports these firewalls for discovery and monitoring.

- Check Point FireWall-1
- Check Point Provider-1
  - CLM for Check Point Provider-1
  - CMA for Check Point Provider-1
  - MDS for Check Point Provider-1
  - MLM for Check Point Provider-1
- Check Point VSX
- Cisco Adaptive Security Appliance (ASA)
- Cisco Firepower Threat Defense (FTD)
- Clavister Firewall
- Cyberoam Firewall
- Dell SonicWALL
- Fortinet FortiGate Firewall
- Imperva SecureSphere Web App Firewall
- Juniper Networks SSG
- McAfee Firewall Enterprise (Sidewinder)
- Palo Alto
- Sophos UTM
- Stormshield Network Security
- UserGate UTM Firewall
- WatchGuard Firebox

Check Point FireWall-1

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Check Point

Product Information: https://www.checkpoint.com/products/

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Firewall model and version, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
LEA		All traffic and system logs	Security and Compliance
Syslog		Traffic and logs sent via the CheckPoint Log Exporter tool via CEF format.	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "firewall-1" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Syslog CEF Format
- LEA

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog CEF Format

The Syslog CEF format is a more straightforward integration method than LEA, and collects similar information. To configure CheckPoint for syslog event forwarding, use the CheckPoint Log Exporter tool that details on how to configure the CheckPoint Firewall at the following URL:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323.

Configure the tool to send Syslog in CEF format to FortiSIEM.

Example CEF Format Log

```
CEF:0|Check Point|VPN-1 & FireWall-1|Check Point|Log|domain-udp|Unknown|act=Accept
deviceDirection=0 rt=1528095651000 spt=49005 dpt=53 cs2Label=Rule Name cs2=Implicit Cleanup
layer_name=LRSK Security layer_name=LRSK Application layer_uuid=ab166dee-e955-4b8f-a5e7-
6234fbaeefde layer_uuid=5549ebc0-70a4-43d1-8ec6-ca53f2306a62 match_id=34 match_id=33554431
parent_rule=0 parent_rule=0 rule_action=Accept rule_action=Accept rule_uid=78f0ba26-4d36-
4352-96dd-0303a2a31cbb ifname=eth2 logid=0 loguid={0x5b14e3a3,0x0,0xfbffff0a,0xc0000008}
origin=1.1.1.1 originsicname=CN\=gate2,O\=pgkeeper.citadele.lrs.lt.wj6ide sequencenum=99
version=5 dst=1.1.1.1 inzone=Internal outzone=Internal product=VPN-1 & FireWall-1 proto=17
service_id=domain-udp src=1.1.1.1
```

LEA

Sending events from Checkpoint to FortiSIEM in Syslog CEF format can be a more straightforward integration method than using LEA Integration method.

Following the steps here for LEA configuration.

- Add FortiSIEM as a Managed Node
- Create an OPSEC Application for FortiSIEM
- Create a Firewall Policy for FortiSIEM

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host...** .
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like `FortiSIEMVA`.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.
4. Enter a **Name** for your OPSEC application, like `OPSEC_FortiSIEMVA`.
5. For **Host**, select the FortiSIEM host.
6. Under **Client Entities**, select **LEA** and **CPMI**.
   For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
   This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like `CN=OPSEC_ FortiSIEMVA,0=MDS..i6g4zq`.
    This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In **Servers and Opsec > OPSEC Applications**, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
   Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.
9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Checkpoint Firewall-1
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Check Point Provider-1 Firewall

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Firewall model and version, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
LEA		All traffic and system logs	Security and Compliance

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration Overview

The configuration of Check Point Provider-1 depends on the type of log that you want sent to FortiSIEM. There are two options:

- **Domain level audit logs**, which contain information such as domain creation, editing, etc.
- **Firewall logs**, which include both audit log for firewall policy creation, editing, etc., and traffic logs

These logs are generated and stored among four different components:

- **Multi-Domain Server (MDS)**, where domains are configured and certificates have to be generated.
- **Multi-Domain Log Module (MLM),** where domain logs are stored.
- **Customer Management Add-on (CMA)**, the customer management module.
- **Customer Log Module (CLM)**, which consolidates logs for an individual customer/domain.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Component Configuration for Domain-Level Audit Logs

1. Configure MDS.
2. Use the **Client SIC** obtained while configuring MDS to configure MLM.
3. Pull logs from MLM.

Component Configuration for Firewall Logs

1. Configure CMA.
2. Use the **Client SIC** obtained while configuring CMA to configure CLM.
3. Pull logs from CLM.
   If you want to pull firewall logs from a domain, you have to configure CLM for that domain.

See these topics for instructions on how to configure each component for Check Point Provider-1 firewalls.

- Configuring MDS for Check Point Provider-1 Firewalls
- Configuring MLM for Check Point Provider-1 Firewalls
- Configuring CMA for Check Point Provider-1 Firewalls
- Configuring CLM for Check Point Provider-1 Firewalls

Configuring CMA for Check Point Provider-1 Firewalls

The Check Point Provider-1 Customer Management Add-On (CMA) creates logs that are then consolidated by the Customer Log Module (CLM). If you want the CLM to send logs to FortiSIEM, you must first configure the CMA and obtain the **AO Client SIC** to configure access credentials for communication between the CLM and FortiSIEM.

- Configuration
- Settings for Access Credentials

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get CMA Server SIC for Setting Up FortiSIEM Access Credentials

1. Log in to your Check Point SmartDomain Manager.
2. Click the **General** tab.
3. Select **Domain Contents**.
4. Select the **Domain Management Server** and right-click to select **Launch Application > Smart Dashboard**.
5. Select the **Desktop** tab.
6. Select the **Network Objects** icon.
7. Double-click on the **Domain Management Server** to view the **General Properties** dialog.
8. Click **Test SIC Status...** .
   Note the value for **DN**. You will use this for the **CMA Server SIC** setting when creating the access credentials for FortiSIEM to access your CMA server.

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host...** .
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like `FortiSIEMVA`.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.
4. Enter a **Name** for your OPSEC application, like `OPSEC_FortiSIEMVA`.
5. For **Host**, select the FortiSIEM host.
6. Under **Client Entities**, select **LEA** and **CPMI**.
   For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
   This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like `CN= OPSEC_ FortiSIEMVA,0=MDS..i6g4zq`.
    This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In Servers and Opsec > OPSEC Applications, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
   Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.
9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall CLA SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point Provider-1 Firewall CMA. When you complete the access credentials, click **Generate Certificate** to establish access between your firewall and FortiSIEM.

Setting	Value
Name	CMA
Device Type	Checkpoint Provider-1 CMA
Access Protocol	CheckPoint SSLCA
CMA IP	The IPS address of your server
Checkpoint LEA Port	The port used by LEA on your server
AO Client SIC	The DN number of your FortiSIEM OPSEC application
CMA Server SIC	The DN number of your server
CPMI Port	The port used by CPMI on your server
Activation Key	The password you used in creating your OPSEC application

Configuring CLM for Check Point Provider-1 Firewalls

- Prequisites
- Configuration
- Settings for Access Credentials

Prequisites

- You must first configure and discover the Check Point CLA and obtain the **AO Client SIC** before you can configure the Customer Log Module (CLM). The AO Client SIC is generated when you create the FortiSIEM OPSEC application.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get CLM Server SIC for Creating FortiSIEM Access Credentials

1. Log in to your Check Point SmartDomain Manager.
2. Click the **General** tab.
3. Select **Domain Contents**.
4. Select the **Domain Management Server** and right-click to select **Launch Application > Smart Dashboard**.
5. Select the **Desktop** tab.
6. Click the **Network Objects** icon.
7. Under **Check Point**, select the CLM host and double-click to open the **General Properties** dialog.
8. Under Secure Internal Communication, click **Test SIC Status...** .
9. In the **SIC Status** dialog, note the value for **DN**.
   This is the CLM Server SIC that you will use in setting up access credentials for the CLM in FortiSIEM.
10. Click **Close**.
11. Click **OK**.

Install the Database

1. In the **Actions** menu, select **Policy > Install Database...** .
2. Select the MDS Server and the CLM, and then **OK**.
   The database will install in both locations.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall CLM SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point Provider-1 Firewall CMA. When you complete the access credentials, click **Generate Certificate** to establish access between your firewall and FortiSIEM.

Setting	Value
Name	CLM
Device Type	Checkpoint Provider-1 CLM
Access Protocol	CheckPoint SSLCA
CLM IP	The IP address of the host where your CLM is located
Checkpoint LEA Port	The port used by LEA on your server
AO Client SIC	The DN number of your FortiSIEM OPSEC application
CLM Server SIC	The DN number of your server
CPMI Port	The port used by CPMI on your server
CMA IP	The IP address of the host where your CMA is located

Configuring MDS for Check Point Provider-1 Firewalls

- Configuration
- Settings for Access Credentials

The Check Point Provider-1 firewall Multi-Domain Server (MDS) is where domains are configured and certificates are generated for communicating with FortiSIEM. If you want to have domain logs from the Multi-Domain Log Module (MLM) sent from your firewall to FortiSIEM, you must first configure and discover MDS, then use the AO Client SIC created for your FortiSIEM OPSEC application to configure the access credentials for MLM.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get the MDS Server SIC for FortiSIEM Access Credentials

You will use the MDS Server SIC to create access credentials in FortiSIEM for communicating with your server.

1. Log in to your Check Point SmartDomain Manager.
2. Select **Multi-Domain Server Contents**.
3. Select **MDS**, and then right-click to select **Configure Multi-Domain Server...** .
4. In the **General** tab, under **Secure Internet Communication**, note the value for **DN**.

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host...** .
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like `FortiSIEMVA`.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.
4. Enter a **Name** for your OPSEC application, like `OPSEC_FortiSIEMVA`.
5. For **Host**, select the FortiSIEM host.

6. Under **Client Entities**, select **LEA** and **CPMI**.
   For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
   This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like `CN= OPSEC_ FortiSIEMVA,0=MDS..i6g4zq`.
    This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In Servers and Opsec > OPSEC Applications, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
   Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.
9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

Copy Secure Internal Communication (SIC) certificates

Copy Client SIC

1. Go to **Manage > Server and OPSEC Applications**.
2. Select **OPSEC Application** and then right-click to select **accelops**.
3. Click **Edit**.
4. Enter the **SIC DN** of your application.

Copy Server SIC

1. In the **Firewall** tab, go to **Manage**.
2. Click the **Network Object** icon, and then right-click to select **Check Point Gateway**.
3. Click **Edit**.
4. Enter the **SIC DN**.
5. If there isn't a field to enter the SIC DN, click **Test SIC Status** and a dialog will display the SIC DN.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point Provider-1 Firewall MDS. When you complete the access credentials, click **Generate Certificate** to establish access between your firewall and FortiSIEM.

Setting	Value
Name	MDS
Device Type	Checkpoint Provider-1 MDS
Access Protocol	CheckPoint SSLCA
MDS IP	The IPS address of your server
Checkpoint LEA Port	The port used by LEA on your server
AO Client SIC	The DN number of your FortiSIEM OPSEC application
MDS Server SIC	The DN number of your server
Password	The password associated with the administrative user
CPMI Port	The port used by CPMI on your server
Activation Key	The password you used in creating your OPSEC application

1. Generate a certificate for MDS communication in FortiSIEM.
    a. Configure Checkpoint Provider-1 MDS credential as shown below.
    Activation key was the one-time password you input in Create an OPSEC Application for FortiSIEM
    AO Client SIC was generated in Create an OPSEC Application for FortiSIEM
    MDS Server SIC was generated in Get the MDS Server SIC for FortiSIEM Access Credentials
    b. Click **Generate Certificate**. It should be successful. Note that the button will be labeled **Regenerate Certificate** if you have already generated the certificate once.

Configuring MLM for Check Point Provider-1 Firewalls

- Prerequisites
- Configuration
- Settings for Access Credentials

Prerequisites

- You must configure and discover your Check Point Provider-1 MDS before you configure the Multi-Domain Log Module (MLM). You will need the **AO Client SIC** that was generated when you created your FortiSIEM OPSEC application in the MDS to set up the access credentials for your MLM in FortiSIEM.

Discover Paired Components on the Same Collector or Supervisor

Discovery of the MLM requires the certificate of the MDS, and discovery of the CLM requires the certificate of the CMA. Make sure that you discover the MDS & MLM pair, and the CMA & CLM pair, on the same Supervisor or Collector. If you attempt to discover them on separate Collectors, discovery will fail.

Configuration

Get MLM Server SIC for Setting Up FortiSIEM Access Credentials

1. Log in to your Check Point SmartDomain Manager.
2. In the **General** tab, click **Multi-Domain Server Contents**.
3. Right-click **MLM** and select **Configure Multi-Domain Server...**.
4. Next to **Communication**, note the value for **DN**.

You can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Settings for Check Point Provider-1 MLM SSLCA Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your Check Point MLM over SSLCA.

Setting	Value
Name	MLM
Device Type	Checkpoint Provider-1 MLM
Access Protocol	CheckPoint SSLCA
MLM IP	The IPS address of your module
Checkpoint LEA Port	The port used by LEA on your server

Setting	Value
AO Client SIC	The DN number of your FortiSIEM OPSEC application
MLM Server SIC	The DN number of your MLM
CPMI Port	The port used by CPMI on your server
MDS IP	The IP address of your MDS server

Check Point VSX Firewall

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

FortiSIEM uses SNMP, LEA to discover the device and to collect logs, configurations and performance metrics.

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Firewall model and version, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
LEA		All traffic and system logs	Security and Compliance

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- LEA

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

LEA

- Add FortiSIEM as a Managed Node
- Create an OPSEC Application for FortiSIEM
- Create a Firewall Policy for FortiSIEM
- Copy Client SIC
- Copy Server SIC

Add FortiSIEM as a Managed Node

1. Log in to your Check Point SmartDomain Manager.
2. In the **Global Policies** tab, select **Multi-Domain Security Management**, and then right-click to select **Launch Global SmartDashboard**.
3. Select the **Firewall** tab.
4. Click the **Network Objects** icon.
5. Select **Nodes**, and then right-click to select **Node > Host...**.
6. Select **General Properties**.
7. Enter a **Name** for your FortiSIEM host, like `FortiSIEMVA`.
8. Enter the **IP Address** of your FortiSIEM virtual appliance.
9. Click **OK**.

Create an OPSEC Application for FortiSIEM

1. In the **Firewall** tab, click the **Servers and OPSEC** icon.
2. Select **OPSEC Applications**, and then right-click to select **New > OPSEC Application**.
3. Click the **General** tab.
4. Enter a **Name** for your OPSEC application, like `OPSEC_FortiSIEMVA`.
5. For **Host**, select the FortiSIEM host.
6. Under **Client Entities**, select **LEA** and **CPMI**.
   For Check Point FireWall-1, also select **SNMP**.
7. Click **Communication**.
8. Enter a one-time password.
   This is the password you will use in setting up access credentials for your firewall in FortiSIEM.
9. Click **Initialize**.
10. Close and re-open the application.
11. In the **General** tab, next to **Communication**, the **DN** field will now contain a value like `CN=OPSEC_FortiSIEMVA,0=MDS..i6g4zq`.
    This is the **FortiSIEM Client SIC DN** that you will need when you copy the secure internal communication certificates and set the access credentials for your firewall in FortiSIEM.

Create a Firewall Policy for FortiSIEM

1. In Servers and Opsec > OPSEC Applications, select your FortiSIEM application.
2. In the **Rules** menu, select **Top**.
3. Right-click **SOURCE**, then click **Add** and select your FortiSIEM virtual appliance.
4. Right-click **DESTINATION**, then click **Add** and select your Check Point firewall.
5. Right-click **SERVICE**, then click **Add** and select **FW1_lea**, and **CPMI**.
   Also select **snmp** if you are configuring a Check Point FireWall-1 firewall.
6. Right-click **ACTION** and select **Accept**.
7. Right-click **TRACK** and select **Log**.
8. Go to **Policy > Install**.
9. Click **OK**.
10. Go to **OPSEC Applications** and select your FortiSIEM application.
11. In the **General** tab of the **Properties** window, make sure that the communications have been enabled between your firewall and FortiSIEM.

Copy Client SIC

1. Go to **Manage > Server and OPSEC Applications**.
2. Select **OPSEC Application** and then right-click to select **accelops**.
3. Click **Edit**.
4. Enter the **SIC DN** of your application.

Copy Server SIC

1. In the **Firewall** tab, go to **Manage**.
2. Click the **Network Object** icon, and then right-click to select **Check Point Gateway**.
3. Click **Edit**.
4. Enter the **SIC DN**.
5. If there isn't a field to enter the SIC DN, click **Test SIC Status** and a dialog will display the SIC DN.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Checkpoint VSX
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco Adaptive Security Appliance (ASA)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	Host name, Hardware model, Network interfaces, Hardware component details: serial number, model, manufacturer, software and firmware versions of components such as fan, power supply, network cards etc., Operating system version, SSM modules such as IPS	Uptime, CPU and Memory utilization, Free processor and I/O memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
SNMP (V1, V2c, V3)		**Hardware health**: temperature, fan and power supply status	
SNMP (V1, V2c, V3)	OSPF connectivity, neighbors, state, OSPF Area	OSPF state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)		**IPSec VPN Phase 1 tunnel metrics**: local and remote Vpn Ip addresses, Tunnel status, Tunnel Uptime, Received/Sent BitsPerSec, Received/Sent Packets, Received/Sent BitsPerSec, Received/Sent Dropped Packets, Received/Sent Rejected Exchanges, Received/Sent Invalid	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
		Exchanges Invalid Received Pkt Dropped, Received Exchanges Rejected, Received **Exchanges Invalid IPSec VPN Phase 2 tunnel metrics**: local and remote Vpn Ip addresses, Tunnel status, Tunnel Uptime, Received/Sent BitsPerSec, Received/Sent Packets, Received/Sent BitsPerSec, Received/Sent Dropped Packets, Received/Sent Auth Failed, Sent Encrypted Failed, Received Decrupt failed, Received Replay Failed	
Telnet/SSH	Running and startup configuration, Interface security levels, Routing tables, Image file name, Flash memory size	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
Telnet/SSH		**Virtual context for multi-context firewalls**, ASA interface security levels needed for setting source and destination IP address in syslog based on interface security level comparisons, ASA name mappings from IP addresses to locally unique names needed for converting names in syslog to IP addresses	
Netflow (V9)	Open server ports	Traffic logs (for ASA 8.x and above)	Security and Compliance
Syslog	Device type	All traffic and system logs	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "asa-" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "asa" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "asa" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- Don't configure SNMP Trap.
- Don't configure ASA to send logs via SNMP trap, as FortiSIEM doesn't parse them.

Check Security Levels

Make sure interface security levels are appropriately set in FortiSIEM. In your FortiSIEM Supervisor, go to **CMDB > Devices > Network Device > Firewall** and select your firewall. Click the **Interface** tab, and make sure that the inside security level is 100, outside is 0 and other interfaces are in between. This information can either be discovered via SSH or entered manually after SNMP discovery. Without correct security level information, ASA traffic built and teardown logs can not be parsed correctly (they may not have correct source and destination addresses and ports).

Configuration topics are listed here.

- SNMP
- Syslog
- Sample Cisco ASA Syslog
- SSH
- Telnet
- Commands Used During Telnet/SSH Communication

SNMP

1. Log in to your ASA with administrative privileges.
2. Configure SNMP with this command.

```
snmp-server host <ASA Interface name> <FortiSIEM IP> poll community <community string>
```

Syslog

1. Log in to your ASA with administrative privileges.
2. Enter configuration mode (config terminal).
3. Enter the following commands:
    - no names
    - logging enable
    - logging timestamp
    - logging monitor errors
    - logging buffered errors
    - logging trap debugging
    - logging debug-trace
    - logging history errors
    - logging asdm errors
    - logging mail emergencies
    - logging facility 16
    - logging host <ASA interface name> <FortiSIEM IP>

Example using Cisco ASA + Anyconnect vpn logging / SNMP

Notes regarding example:

Replace content marked with <*italicized_text*> with your actual content.

Replace “inside” with the egress firewall zone that logging traffic is sent

Avoid whitespace in your passwords, group name, and username.

```
logging enable
logging timestamp
no logging hide username
logging host inside <IP_address_of_your_FortiSIEM_collector>
logging class auth trap informational
logging class config trap informational
logging class vpn trap informational
logging class vpnc trap debugging
logging class webvpn trap informational
logging class svc trap informational

snmp-server enable
snmp-server group <SNMP_group_name> v3 priv
snmp-server user <Your_chosen_SNMPv3_username> <SNMP_group_name> v3 auth sha <Your_SHA_
password> priv aes 128 <Your_AES_Password>
snmp-server host inside <IP_address_of_your_FortiSIEM_collector> poll version 3 <Your_
chosen_SNMPv3_username>
```

Sample Cisco ASA Syslog

```
<134>Nov 28 2007 17:20:48: %ASA-6-302013: Built outbound TCP connection 76118 for
outside:207.68.178.45/80 (207.68.178.45/80)
to inside:192.168.20.31/3530 (99.129.50.157/5967)
```

SSH

1. Log in to your ASA with administrative privileges.
2. Configure SSH with this command.

   ```
   ssh <FortiSIEM IP>  <FortiSIEM IP netmask>  <ASA interface name>
   ```

Telnet

1. Log in to your ASA with administrative privileges.
2. Configure telnet with this command.

   ```
   telnet <FortiSIEM IP>  <FortiSIEM IP netmask>  <ASA interface name>
   ```

Commands Used During Telnet/SSH Communication

The following commands are used for discovery and performance monitoring via SSH. Make sure that the accounts associated with the ASA access credentials you set up in FortiSIEM have permission to execute these commands.

Critical Commands

It is critical to have `no names` and `logging timestamp` commands in the configuration, or logs will not be parsed correctly.

1. `show startup-config`
2. `show running-config`
3. `show version`
4. `show flash`
5. `show context`
6. `show ip route`
7. `enable`
8. `terminal pager 0`
9. `terminal length 0`

NetFlow

NetFlow is an optimized protocol for collecting high volume traffic logs. You should configure NetFlow with ASM, the ASA device manager.

- Set Up FortiSIEM as a NetFlow Receiver
- Create a NetFlow Service Policy
- Configure the Template Refresh Rate

Set Up FortiSIEM as a NetFlow Receiver

1. Login to ASDM.
2. Go to **Configuration > Device Management > Logging > Netflow**.
3. Under Collectors, click **Add**.
4. For **Interface**, select the ASA interface over which NetFlow will be sent to FortiSIEM.
5. For **IP Address or Host Name**, enter the IP address or host name for your FortiSIEM virtual appliance that will receive the NetFlow logs.
6. For **UDP Port**, enter **2055**.
7. Click **OK**.
8. Select **Disable redundant syslog messages**.
   This prevents the netflow equivalent events from being also sent via syslog.
9. Click **Apply**.

Create a NetFlow Service Policy

1. Go to **Configuration > Firewall > Service Policy Rules**.
2. Click **Add**.
   The **Service Policy Wizard** will launch.
3. Select **Global - apply to all interfaces**, and then click **Next**.
4. For **Traffic Match Criteria**, select **Source and Destination IP Address**, and then click **Next**.
5. For **Source** and **Destination**, select **Any**, and then click **Next**.
6. For **Flow Event Type**, select **All**.
7. For **Collectors**, select the FortiSIEM virtual appliance IP address.
8. Click **OK**.

Configure the Template Refresh Rate

This is an optional step. The template refresh rate is the number of minutes between sending a template record to FortiSIEM. The default is 30 minutes, and in most cases this is sufficient. Since flow templates are dynamic, FortiSIEM cannot process a flow until it knows the details of the corresponding template. This command may not always be needed, but if flows are not showing up in FortiSIEM, even if `tcpdump` indicates that they are, this is worth trying.

```
flow-export template timeout-rate 1
```

You can find out more about configuring NetFlow in the Cisco support forum.

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Cisco Firepower Threat Defense (FTD)

- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Comparison of Syslog and eStreamer for Security Eventing

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco-ftd" to see the event types associated with this device.

Rules

There are no specific rules available for Cisco Firepower Threat Defense. Matches device agnostic firewall rules.

Reports

There are no specific reports available for Cisco Firepower Threat Defense. Matches device agnostic firewall rules.

Configuration

Before configuring, you may want to see a comparison of Syslog and eStreamer for Security Eventing first.

FirePower Threat Defense SNMP Configuration through Firepower Management Center

Cisco Firepower Threat Defense (FTD) supports SNMPv1, v2c, and SNMPv3. Take the following steps to configure:

1. Login to the Firepower Management Center (FMC) GUI, and navigate to **Devices > Platform Settings > (Policy) > SNMP**.
2. Check the **Enable SNMP Servers** checkbox, and configure the SNMPv2 settings.

3. Click on the **Hosts** tab.
4. Click on **Add**, and specify your SNMP server settings in the **Add SNMP Management Hosts** window.
5. Deploy the policy.

For the latest configuration instructions and information, see **Configuring SNMP for FTD** at https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/white-paper-c11-741739.html.

FirePower Threat Defense Syslog Configuration through Firepower Management Center

To configure Syslog, take the following steps:

1. Login to the Firepower Management Center (FMC) GUI, and navigate to **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.
2. Click **Add** to add a Logging Filter for a specific logging destination.
3. From the **Logging Destination** drop-down list, choose the logging destination.

For the latest configuration instructions and information, see https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200479-Configure-Logging-on-FTD-via-FMC.html.

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic

Setting	Value
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Comparison of Syslog and eStreamer for Security Eventing

The following content is taken from https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/analyze_events_using_external_tools.html#id_102110.

Generally, organizations that do not currently have significant existing investment in eStreamer should use syslog rather than eStreamer to manage security event data externally.

Syslog	eStreamer
No customization required	Significant customization and ongoing maintenance required to accommodate changes in each release
Standard	Propriety
Sends directly from devices	Sends from FMC, adding processing overhead
Support for file and malware events, connection events (including security intelligence events) and intrusion events.	Support for all event types listed in eStreamer Server Streaming.
Some event data can be sent only from FMC. See Data	Includes data that cannot be sent via syslog directly from

Syslog	eStreamer
Sent Only via eStreamer, Not via Syslolog.	devices. See Data Send Only via eStreamer, Not via Syslog.

Clavister Firewall

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
syslog	Host name, Reporting IP	None	Connection – permit and deny, system events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Clavister" to see the event types associated with this device.

Rules

No specific rules are written for Clavister firewall but generic firewall rules will apply.

Reports

No specific reports are written for Clavister firewall but generic firewall rules will apply.

Configuration

Configure Clavister firewall to send logs to FortiSIEM in the supported format (see Sample Events).

Settings for Access Credentials

None required

Sample Events

```
<134>[2016-04-26 16:10:07] EFW: CONN: prio=1 id=00600005 rev=1 event=conn_close_natsat
action=close rule=if3_net_nat_out conn=close connipproto=TCP connrecvif=If3
connsrcip=192.168.99.13 connsrcport=43347 conndestif=If1 conndestip=1.1.1.1 conndestport=443
connnewsrcip=1.1.1.2 connnewsrcport=65035 connnewdestip=1.1.1.1 connnewdestport=443
origsent=1395 termsent=5763 conntime=83
```

```
<134>[2016-04-26 16:10:11] EFW: ALG: prio=1 id=00200001 rev=1 event=alg_session_open
algmod=ftp algsesid=95238 connipproto=TCP connrecvif=If1 connsrcip=1.1.1.3 connsrcport=59576
conndestif=core conndestip=1.1.1.4 conndestport=21 origsent=100 termsent=44
```

```
<134>[2016-04-26 16:10:05] EFW: IPSEC: prio=1 id=01800211 rev=2 event=reconfig_IPsec
action=ipsec_reconfigured
```

Cyberoam Firewall

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Setting for Access Credentials
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Connection – permit and deny, system events, malware events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Cyberoam" to see the event types associated with this device.

Rules

No specific rules are written for Cyberoam firewall but generic firewall rules will apply.

Reports

No specific reports are written for Cyberoam firewall but generic firewall rules will apply.

Configuration

Configure Cyberoam firewall to send logs to FortiSIEM in the supported format (see Sample Events).

Settings for Access Credentials

None required.

Sample Events

```
<30>date=2019-07-10 time=11:06:48 timezone="GMT" device_name="CR50iNG" device_
      id=C162213098933-QQ6REI
log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed"
```

```
status="Allow" priority=Information duration=0 fw_rule_id=12 user_name="" user_gp="" iap=1
ips_policy_id=0 appfilter_policy_id=1 application="" application_risk=0 application_
     technology=""
application_category="" in_interface="PortA" out_interface="" src_mac=00: 0:00: 0:10: 0
src_ip=10.0.70.17 src_country_code=AP dst_ip=1.1.1.1 dst_country_code=IRL protocol="TCP"
src_port=61244 dst_port=443 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip=
     tran_src_port=0
tran_dst_ip=10.0.0.13 tran_dst_port=8080 srczonetype="LAN" srczone="ZONE1"
dstzonetype="WAN" dstzone="WAN" dir_disp="" connevent="Start" connid="3340934816" vconnid=""
```

Dell SonicWALL Firewall

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Hardware model, Network interfaces, Operating system version	CPU Utilization, Memory utilization and Firewall Session Count	Availability and Performance Monitoring
Syslog	Device type	All traffic and system logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "sonicwall" to see the event types associated with Dell SonicWALL firewalls.

Rules

There are no predefined rules for Dell SonicWALL firewalls.

Reports

There are no predefined reports for Dell SonicWALL firewalls.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the

User Guide.

- Dell SonicWALL Firewall Administrator's Guide (PDF)

Syslog

1. Log in to your SonicWALL appliance.
2. Go to **Log > Syslog**.
   Keep the default settings.
3. Under **Syslog Servers**, click **Add**.
   The Syslog Settings wizard will open.
4. Enter the **IP Address** of your FortiSIEM Supervisor or Collector.
   Keep the default **Port** setting of **514**.
5. Click **OK**.
6. Go to **Firewall > Access Rules**.
7. Select the rule that you want to use for logging, and then click **Edit**.
8. In the **General** tab, select **Enable Logging**, and then click **OK**.
   Repeat for each rule that you want to enable for sending syslog to FortiSIEM.

Your Dell SonicWALL firewall should now send syslog to FortiSIEM.

Example Syslog

```
Jan  3 13:45:36 192.168.5.1 id=firewall sn=000SERIAL time="2007-01-03 14:48:06" fw=1.1.1.1
pri=6 c=262144 m=98
msg="Connection Opened" n=23419 src=2.2.2.2:36701:WAN dst=1.1.1.1:50000:WAN proto=tcp/50000
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Fortinet FortiGate Firewall

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuring FortiSIEM through FortiOS REST API
- Configuring SNMP v1 or v2 on FortiGate
- Configuring SNMP v3 on FortiGate
- Configuring SSH on FortiSIEM to communicate with FortiGate
- Configuring FortiSIEM for SNMP and SSH to FortiGate
- Configuring FortiAnalyzer to send logs to FortiSIEM
- Configuring FortiGate to send Netflow via CLI
- Configuring FortiGate to send Application names in Netflow via GUI
- Example of FortiGate Syslog parsed by FortiSIEM

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths). For 5xxx series firewalls, per CPU utilization (event PH_DEV_MON_FORTINET_PROCESSOR_USGE)	Availability and Performance Monitoring
Telnet/SSH	Running configuration	Configuration Change	Performance Monitoring, Security and Compliance
Syslog	Device type	All traffic and system logs	Availability, Security and Compliance
Netflow		Firewall traffic, application detection and application link usage metrics	Security monitoring and compliance, Firewall Link Usage and Application monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortigate" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortigate" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "fortigate" in the main content panel **Search...** field to see the reports associated with this device.

Configuring FortiSIEM through FortiOS REST API

Take the following steps to configure FortiGate for FortiSIEM via the FortiOS REST API.
Note: When upgrading FortiOS, make sure to re-generate the API token in FortiGate and update the FortiSIEM Access Credentials information.

- Setup of FortiGate
- Setup of FortiSIEM

Setup of FortiGate

As an administrator with the super_admin profile, login to the FortiGate GUI and take the following steps:

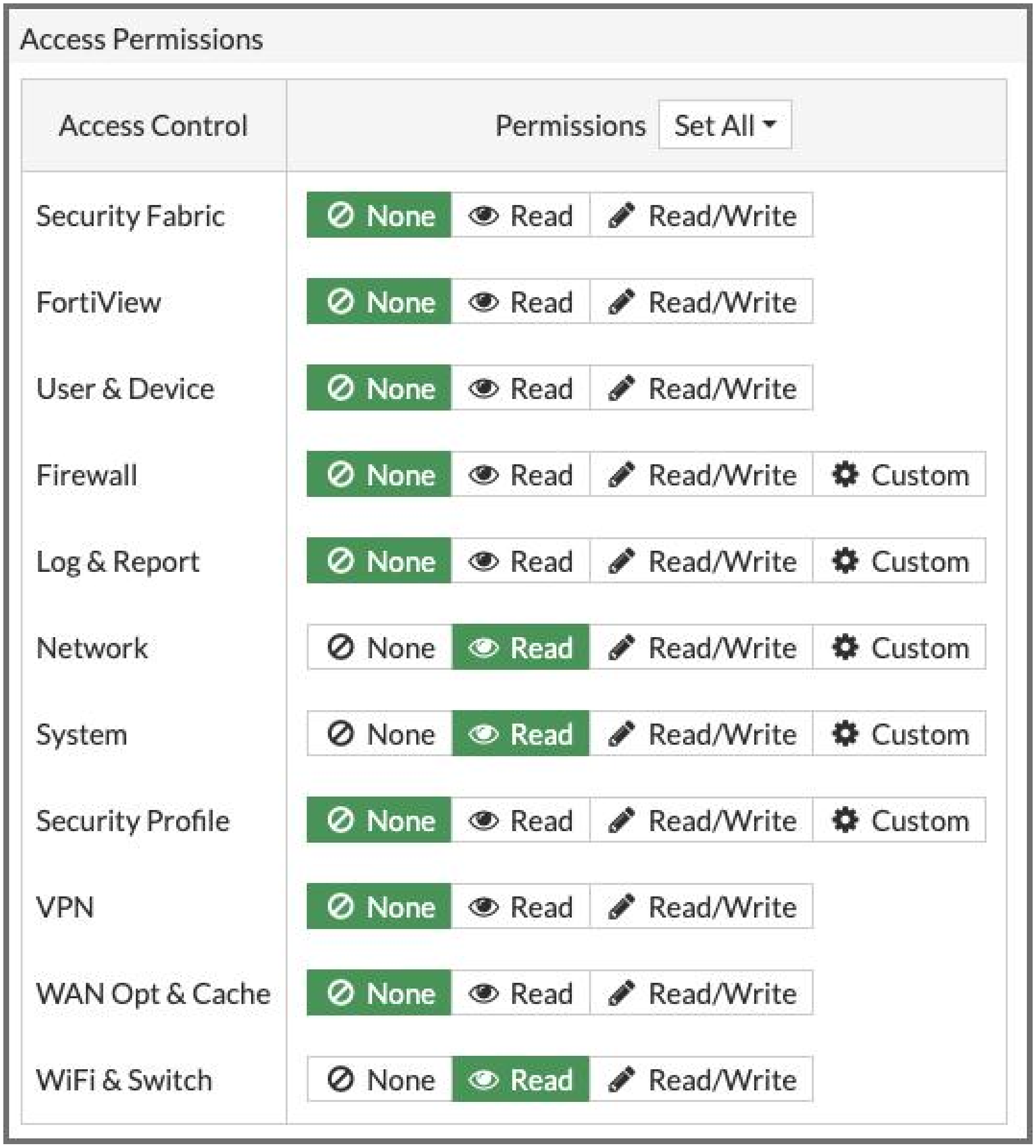
Step 1: Identify your Source Address

First, identify your source IP address. The source address is needed to ensure the API token can only be used from trusted hosts. If you already know your trusted host IP address, skip to Step 2.

1. On the FortiGate GUI, select the **Status** dashboard and locate the **Administrators** widget.
2. Navigate to **<*your-userid*> > Show active administrator sessions**.
3. Copy the Source Address for your <*your-userid*>. This information will be needed to create the Trusted Host in Step 3: Create the REST API Admin.

Step 2: Create an Administrator Profile

1. On the FortiGate GUI, navigate to **System > Admin Profiles > Create New**.
2. For **Network**, **System**, and **WiFi & Switch** fields, enable **Read** permission.



Access Permissions

Access Control	Permissions Set All ▾
Security Fabric	[✓ None] Read Read/Write
FortiView	[✓ None] Read Read/Write
User & Device	[✓ None] Read Read/Write
Firewall	[✓ None] Read Read/Write Custom
Log & Report	[✓ None] Read Read/Write Custom
Network	None [✓ Read] Read/Write Custom
System	None [✓ Read] Read/Write Custom
Security Profile	[✓ None] Read Read/Write Custom
VPN	[✓ None] Read Read/Write
WAN Opt & Cache	[✓ None] Read Read/Write
WiFi & Switch	None [✓ Read] Read/Write

3. Click **OK**.

Step 3: Create the REST API Admin

1. On the FortiGate GUI, navigate to **System > Administrators > Create New > REST API Admin**.
2. On the **New REST API Admin** dialog, enter the following information.
   a. In the **Username** field, enter a user name.
   b. (Optional) In the **Comments** field, enter any additional information about this account.
   c. In the **Administrator Profile** drop-down list, select the profile from Step 2.

d. Disable **PKI Group**.
e. Enable **CORS Allow Origin**, and input `https://fndn.fortinet.net`.
f. In the **Trusted Hosts** field, enter a trusted host based off your source address. The Trusted Host must be specified to ensure that your local host can reach FortiGate. For example, to restrict requests as coming from only 10.20.100.99, enter "10.20.100.99/32". The Trusted Host is created from the Source Address obtained in Step 1: Identify your Source Address.
g. Click **OK** and an API token will be generated. Copy the API token information as it is only shown once and cannot be retrieved. It will be needed for the Setup in FortiSIEM configuration.
h. Click **Close** to complete the creation of the REST API Admin.

Setup in FortiSIEM

FortiSIEM can process events from FortiGate via the FortiOS REST API. Obtain your token from FortiGate (see Setup in FortiGate) before proceeding.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Fortinet FortiOS
Access Protocol	FORTIOS_REST_API
Password config	Manual
Token	Input the API token from Step 3: Create the REST API Admin in Setup of FortiGate.
Confirm Token	Input the same API token as above for verification.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter the FortiGate IP address or IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiGate.
5. Navigate to **ADMIN > Setup > Discover > New**.
6. In the **Discovery Definition** window, take the following steps:
   a. In the **Name** field, enter a name for this device.
   b. In the **Discovery** Type drop-down list, select Range Scan.
   c. In the **Include** field, enter the FortiGate IP address.
   d. Click **Save**.
7. Navigate to **ADMIN > Setup > Discovery > Discover**. Your devices will be added into CMDB and 3 jobs are added in Monitor Performance.

When configuration is complete, you can do the following.

To view your devices, go to **CMDB > Devices**.

To see metrics for your devices, go to **ADMIN > Setup > Monitor Performance**.

To see received events, select **ANALYTICS**, then enter "PH_DEV_MON_FORTI" in the search box.

Configuring SNMP v1 or v2 on FortiGate

Follow these steps to configure SNMPv1 or v2 on FortiGate. For more information on configuring the FortiGate to allow detailed interface monitoring using SNMP, see Data Source in the FortiSIEM User's Guide.

1. Log in to your firewall as an administrator.
2. Go to **System** > **Network**.
3. Select the FortiGate interface IP that FortiSIEM will use to communicate with your device, and then click **Edit**.
4. For **Administrative Access**, makes sure that **SSH** and **SNMP** are selected.
5. Click **OK**.
6. Go to **System** > **Config** > **SNMP v1/v2c**.
7. Click **Create New** to enable the `public` community.

Configuring SNMP v3 on FortiGate

To configure SNMPv3 on a FortiGate Firewall and integrate it with FortiSIEM, take the following steps:

Setup for FortiGate

1. Allow SNMP traffic on inbound interface where FortiSIEM collector will reach FortiGate firewall.
2. Run the `show` command under the interface, then run "set allowaccess option1 option2 snmp", replacing the options with the preexisting values, adding snmp to the end.

   The following example has the FortiSIEM collector polling inbound on interface port 1.

```
config system interface

edit "port1"

 show

 set allowaccess snmp

end

config system snmp sysinfo

 set status enable

 set description "Description of device"

 set contact-info "Optional contact info"

 set location "Optional location info"

end
```

3. Replace the sha and aes passwords with your own, and for notify-hosts, enter the IP address of your FortiSIEM collector that will be polling the FortiGate unit.

```
config system snmp user
edit "fortisiem_user"
 set status enable
 set queries enable
 set security-level auth-priv
 set auth-proto sha
 set auth-pwd "yourShaPassword1"
 set priv-proto aes
 set priv-pwd "yourAesPassword1"
 set notify-hosts "192.168.1.2"
 next
end
```

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Generic
Access Protocol	SNMP v3
Security Level	authPriv
Security Name	fortisiem_user or <*your SNMPv3 username here*>
Auth Protocol	SHA
Auth Password	<*your password*>
Priv Protocol	AES
Priv Password	<*your password*>
Context	You can leave this field blank.
Description	Optional, you can explain which devices this credential is used for.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   Note: If multiple collectors, use the collector drop-down list to select which collector will do the polling. If you have

only 1 collector, no drop-down list will appear.

a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field. You can add multiple IPs by using a comma as a separator, for example:
   192.168.1.1,192.168.2.1,192.168.3.1
b. Select the name of your credential from the **Credentials** drop-down list.
c. Click **Save**.

4. Click the **Test** drop-down list and select **Test Connectivity without Ping** to test the connection. If it fails, ensure the firewall is configured correctly, that SNMP is allowed from the collector on UDP 161, and that the correct SNMPv3 user and password is being used.
5. Click the **Discovery** tab. If there is more than one collector, select from the drop-down list the collector you'd like to do the polling.
6. In the include list, enter the same comma separated IP list as before.
7. Optionally, you can disable ICMP alive check by selecting **Options > Do not ping before discovery**.
8. Click **Save**.
9. Select the new discovery, and click **Discover**. Wait for it to finish, or click run in background.
10. Click the **CMDB** tab, and confirm that the devices are discovered via SNMP.

Configuring SSH on FortiSIEM to communicate with FortiGate

FortiSIEM Collector SSH Client, when communicating to FortiGate via SSH, may use the public key authentication method first. This may fail and create some alerts in FortiGate. To prevent this, modify the per user config file as follows:

1. Log in to the FortiSIEM node that communicates to FortiGate via SSH, as `admin`.
2. Open `/opt/phoenix/bin/.ssh/config` and create a new file, if necessary.
3. Add these two lines and save:

```
PreferredAuthentications password
PubkeyAuthentication no
```

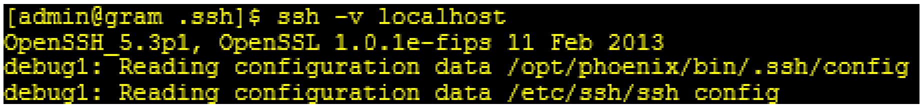
4. Ensure that the owner is admin:

```
chown admin.admin /opt/phoenix/bin/.ssh/config
chmod 600 /opt/phoenix/bin/.ssh/config
```

5. Verify using the commands:

```
su admin
ssh -v <fgt host>
```

Verification is successful if the following files are found:



```
[admin@gram .ssh]$ ssh -v localhost
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
debug1: Reading configuration data /opt/phoenix/bin/.ssh/config
debug1: Reading configuration data /etc/ssh/ssh_config
```

Alternatively, modify the `global ssh_config` file as below. Since this is a global configuration, all programs will use this setting.

1. Log in to a FortiSIEM node that communicates to FortiGate via SSH, as `root`.
2. Open `/etc/ssh/ssh_config`
3. Add these two lines:

```
                     PreferredAuthentications password
                     PubkeyAuthentication no
```

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

```
show firewall address
```

```
show full-configuration
```

Sending Logs Over VPN

If you are sending these logs across a VPN, Fortigate will try to use the WAN interface for the `source` of all system traffic. You can change this by setting the `source-ip` option to the IP used on the Fortigates Internal/LAN interface.

With the Web GUI

1. Log in to your firewall as an administrator.
2. Go to **Log & Report** > **Log Config** > **syslog**.
3. Enter the **IP Address**, **Port Number**, and **Minimum Log Level and Facility** for your FortiSIEM virtual appliance.
4. Make sure that **CSV format** is not selected.

With the CLI

1. Connect to the Fortigate firewall over SSH and log in.
2. To configure your firewall to send syslog over UDP, enter this command, replacing the IP address `192.168.53.2` with the IP address of your FortiSIEM virtual appliance.

   ```
   config log syslogd setting
       set status enable
       set server "192.168.53.2"    set facility user
          set port 514
   end
   ```

3. Verify the settings.

   ```
   frontend # show log syslogd setting
   config log syslogd setting
       set status enable
       set server "192.168.53.2"    set facility user
   end
   ```

Configuring FortiSIEM for SNMP and SSH access to FortiGate

You can now configure FortiSIEM to communicate with your device by following the instructions in the *User Guide* > *Section: Configuring FortiSIEM* > *Discovering Infrastructure* > *Setting Access Credentials for Device Discovery*, and then initiate discovery of the device as described in the topics under *Discovering Infrastructure*.

Configuring FortiAnalyzer to send logs to FortiSIEM

Setting Up the Syslog Server

1. Login to FortiAnalyzer.
2. Go to **System Settings** > **Advanced** > **Syslog Server**.
    a. Click the **Create New** button.
    b. Enter the **Name**. (It is recommended to use the name of the FortiSIEM server.)
    c. Fill in the **IP address** (or **FQDN**) with the IP or a fully qualified name of the FortiSIEM server.
    d. Leave the **Syslog Server Port** to the default value '514'.
    e. Click **OK** to save your entries.

Pre-Configuration for Log Forwarding

To configure FortiAnalyzer event forwarding to FortiSIEM, you must first set up the following.

1. 1. Install a FortiSIEM collector in the same subnet as FortiAnalyzer that will be forwarding the events.
   Note: The same subnet request is required as FortiAnalyzer will later be configured to spoof packets to the collector. RPF (reverse path forwarding checks) on network equipment would have to be disabled if FortiAnalyzer and collector existed on different subnets.
2. 2. It is recommended that for every 5,000 EPS (events per second) ingested, you add 1 collector that is 8vCPU, 8GB RAM. If you have more than 5,000 EPS forwarding from FortiAnalyzer, please set up a load balancer with multiple collectors behind it, allowing UDP 514 inbound.

Configuring Log Forwarding

Take the following steps to configure log forwarding on FortiAnalyzer.

1. Go to **System Settings > Log Forwarding**.
2. Click the **Create New** button in the toolbar. The **Create New Log Forwarding** pane opens.
3. fill in the information as per the below table, then click **OK** to create the new log forwarding. The FortiAnalyzer device will start forwarding logs to the server.

Field	Input
Name	FortiSIEM-Forwarding
Status	On
Remote Server Type	Syslog
Compression	OFF

Field	Input
Sending Frequency	Real-time
Log Forwarding Filters	Select all desired Administrative Domains (ADOMs) / device logs you'd like to forward

4. Go to the CLI Console and configure the CLI only log forward option by running the following CLI commands.
   Notes:
   - Logs received by FortiAnalyzer, and then forwarded to FortiSIEM, have the source IP of the log packet overwritten with the IP address of the FortiAnalyzer appliance. This hides the “true” source of the log packet from FortiSIEM. To override this behavior, FortiAnalyzer can spoof the original log sender's IP address when forwarding to FortiSIEM. This allows FortiSIEM collectors to receive all the original information as if it received the logs directly from the originating device.
   - For FortiAnalyzer versions 6.0 and later, use the following CLI:
     Note: Replace <*id*> with the actual name of the log forward created earlier.

     ```
     config system log-forward
         edit <id>
             set mode forwarding
             set fwd-max-delay realtime
             set server-name "<FSM_Collector>"
             set server-ip "a.b.c.d"
             set fwd-log-source-ip original_ip
             set fwd-server-type syslog
         next
     end
     ```

   - For FortiAnalyzer versions 5.6 to 5.9, use the following CLI:
     Note: Replace <*id*> with the actual name of the log forward created earlier.

     ```
     config system log-forward

       edit <id>

        set mode forwarding

        set fwd-max-delay realtime

        set server-ip "a.b.c.d"

        set fwd-log-source-ip original_ip

        set fwd-server-type syslog

      next

     end
     ```

   - For FortiAnalyzer versions earlier than 5.6, use the following CLI:
     Note: For <*id*>, you can choose the number for your FortiSIEM syslog entry.

     ```
     config system aggregation-client

       edit <id>

         set fwd-log-source-ip original_ip

     end
     ```

Configuring FortiSIEM Collector to Receive Logs from FortiAnalyzer

To configure the FortiSIEM collector to receive logs from FortiAnalyzer, you will need to disable RPF checks that would normally cause the collector virtual machine from dropping the log packet as it is spoofed.

```
sysctl -w net.ipv4.conf.all.rp_filter=0
```

To make this change persistent across reboots, add the following code to the `/etc/sysctl.conf` file.

```
echo “net.ipv4.conf.all.rp_filter=0”
```

1.
   - `end`

Configuring FortiGate to send Netflow via CLI

1. Connect to the Fortigate firewall over SSH and log in.
2. To configure your firewall to send Netflow over UDP, enter the following commands:
   ```
   config system netflow
   set collector-ip <FortiSIEM IP>
   set collector-port 2055
   end
   ```
3. Enable Netflow on the appropriate interfaces, replacing `port1` with your interface name:
   ```
   config system interface
   edit port1
   set netflow-sampler both
   end
   ```
4. *Optional* - Using Netflow with VDOMs
   For VDOM environments, excluding the management VDOM, Netflow must be configured using the following CLI commands:
   ```
   con global
   con sys netflow
   set collector-ip <FortiSIEM IP>
   set collector-port 2055
   set source-ip <source-ip>
   end
   end

   con vdom
   edit root (root is an example, change to the required VDOM name.)
   con sys interface
   edit wan1 (change the interface to the one to use.)
   set netflow-sampler both
   end
   end
   ```

Configuring FortiGate to send Application names in Netflow via GUI

1. Login to FortiGate.
2. Go to **Policy & Objects** > **IPv4 Policy**.

3. Click on the Policy IDs you wish to receive application information from.
4. Add SSL inspection and App Control on the policy by clicking the **+** button in the Security Profiles column.

Example of FortiGate Syslog parsed by FortiSIEM

```
<185>date=2010-04-11 time=20:31:25 devname=APS3012404200944 device_id=APS3012404200944 log_
id=0104032002 type=event subtype=admin
pri=alert vd=root user="root" ui=ssh(10.1.20.21) action=login status=failed reason="name_
invalid"msg="Administrator root login failed from ssh(10.1.20.21) because of invalid user
name"
```

Imperva SecureSphere Web App Firewall

- Configuration

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create Imperva SecureSphere Web App Firewall credential.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	<set name>
Device Type	Imperva Securesphere Web App Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration
User Name	A user who has access credentials for the device
Password	The password for the user
Super Password	Password for Super

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping for your Imperva SecureSphere Web App Firewall credential.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials**drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Imperva SecureSphere Web App Firewall.
5. To see the jobs associated with Imperva, navigate to **ADMIN > Setup > Pull Events**.
6. To see the received events, select **ANALYTICS**, then enter "Imperva" in the search box.

Juniper Networks SSG Firewall

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
Telnet/SSH	Running configuration	Configuration Change	Performance Monitoring, Security and Compliance
Syslog	Device type	Traffic log, Admin login activity logs, Interface up/down logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Juniper-SSG" and "Juniper_SSG" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP and SSH
- Syslog
- Sample Parsed FortiGate Syslog

SNMP and SSH

Enable SNMP, SSH, and Ping

1. Log in to your firewall's device manager as an administrator.
2. Go to **Network > Interfaces > List**.
3. Select the interface and click **Edit**.
4. Under **Service Options**, for **Management Services**, select **SNMP** and **SSH**.
5. For **Other Services**, select **Ping**.

Create SNMP Community String and Management Station IP

1. Go to **Configuration > Report Settings > SNMP**.
2. If the `public` community is not available, create it and provide it with read-only access.
3. Enter the **Host IP** address and **Netmask** of your FortiSIEM virtual appliance.
4. Select the Source Interface that your firewall will use to communicate with FortiSIEM.
5. Click **OK**.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, see "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

Modify Policies so Traffic Matching a Policy is Sent via Syslog to FortiSIEM

1. Go to **Policies**.
2. Select a policy and click **Options**.
3. Select **Logging**.
4. Click **OK**.

Set FortiSIEM as a Destination Syslog Server

1. Go to **Configuration > Report Settings > Syslog**.
2. Select **Enable syslog messages**.
3. Select the **Source Interface** that your firewall will use to communicate with FortiSIEM.
4. Under **Syslog servers**, enter the **IP/Hostname** of your FortiSIEM virtual appliance.
5. For **Port**, enter **514**.
6. For **Security Facility**, select **LOCALD**.
7. For **Facility**, select **LOCALD**.
8. Select **Event Log** and **Traffic Log**.

9. Select **Enable**.
10. Click **Apply**.

Set the Severity of Syslog to Send to FortiSIEM

1. Go to **Configuration > Report Setting > Log Settings**.
2. Click **Syslog**.
3. Select the **Severity Levels** of the syslog you want sent to FortiSIEM.
4. Click **Apply**.

Sample Parsed FortiGate Syslog

```
<129>Aug 26 11:09:45 213.181.33.233 20090826, 6219282, 2009/08/26 09:09:40, 2009/08/26
08:09:49, global.CoX, 1363,
CoX-eveTd-fw1, 213.181.41.226, traffic, traffic log, untrust, (NULL), 81.243.104.82, 64618,
81.243.104.82,
64618, dmz, (NULL), 213.181.36.162, 443, 213.181.36.162, 443, tcp, global.CoX, 1363,
Workaniser_cleanup, fw/vpn, 34,
accepted, info, no, (NULL), (NULL), (NULL), (NULL), 3, 858, 1323, 2181, 0, 0, 14, 1, no, 0,
Not

<129>Aug 26 11:09:45 213.181.33.233 20090826, 6219282, 2009/08/26 09:09:40, 2009/08/26
08:09:49, global.CoX, 1363,
CoX-eveTd-fw1, Category, Sub-Category, untrust, (NULL), 81.243.104.82, 64618, 81.243.104.82,
64618, dmz,
(NULL), 213.181.36.162, 443, 213.181.36.162, 443, tcp, global.Randstad, 1363, Workaniser_
cleanup, fw/vpn, 34, accepted,
info, no, (NULL), (NULL), (NULL), (NULL), 3, 858, 1323, 2181, 0, 0, 14, 1, no, 0, Not
```

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

McAfee Firewall Enterprise (Sidewinder)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "sidewinder" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Sample Parsed Sidewinder Syslog

```
Jun 18 10:34:08 192.168.2.10 wcrfw1 auditd: date="2011-06-18 14:34:08 +0000",fac=f_http_
proxy,area=a_libproxycommon,
type=t_nettraffic,pri=p_
major,pid=2093,logid=0,cmd=httpp,hostname=wcrfw1.community.int,event="session end",app_
risk=low,
app_categories=infrastructure,netsessid=1adc04dfcb760,src_
geo=US,srcip=74.70.205.191,srcport=3393,srczone=external,protocol=6,
dstip=10.1.1.27,dstport=80,dstzone=dmz1,bytes_written_to_client=572,bytes_written_to_
server=408,rule_name=BTC-inbound,
cache_hit=1,start_time="2011-06-18 14:34:08 +0000",application=HTTP
```

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	McAfee Sidewinder Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Palo Alto Firewall

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Parsed Palo Alto Syslog Message
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Firewall connection count	Availability and Performance Monitoring
Telnet/SSH	Running configuration	Configuration Change	Performance Monitoring, Security and Compliance
Syslog	Device type	Traffic log, Threat log (URL, Virus, Spyware, Vulnerability, File, Scan, Flood and data subtypes), config and system logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "palo alto" to see the event types associated with this device. In 6.3.0, the Palo Alto parser has been enhanced to handle some firewall generated Palo Alto Wildfire log events.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "palo alto" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP, SSH, and Ping

1. Log in to the management console for your firewall with administrator privileges.
2. In the **Device** tab, click **Setup**.
3. Click **Edit**.
4. Under **MGMT Interface Services**, make sure **SSH**, **Ping**, and **SNMP** are selected.
5. For **SNMP Community String**, enter `public`.
6. If there are entries in the **Permitted IP** list, **Add** the IP address of your FortiSIEM virtual appliance.
7. Click **OK**.
8. Go to **Setup > Management** and check that SNMP is enabled on the management interface.

Syslog

Set FortiSIEM as a Syslog Destination

1. Log in to the management console for your firewall with administrator privileges.
2. In the **Device** tab, go to **Log Destinations > Syslog**.
3. Click **New**.
4. Enter a **Name** for your FortiSIEM virtual appliance.
5. For **Server**, enter the IP address of your virtual appliance.
6. For **Port**, enter **514**.
7. For **Facility**, select **LOG_USER**.
8. Click **OK**.

Set the Severity of Logs to Send to FortiSIEM

1. In the **Device** tab, go to **Log Settings > System**.
2. Click **Edit...**.
3. For each type of log you want sent to FortiSIEM, select the FortiSIEM virtual appliance in the **Syslog** menu.
4. Click **OK**.

Create a Log Forwarding Profile

1. In the **Objects** tab, go to **Log Forwarding > System**.
2. Create a new log forwarding profile by entering a **Name** for the profile, and then setting **Syslog** to the IP address of your FortiSIEM virtual appliance for each type of log you want send to FortiSIEM.
3. Click **OK**.

Use the Log Forwarding Profile in Firewall Policies

1. In the **Policies** tab, go to **Security > System**.
2. For each security rule that you want to send logs to FortiSIEM, click **Options**.
3. For **Log Forwarding Profile**, select the profile you created for FortiSIEM.
4. Click **OK**.
5. Commit changes.

Logging Permitted Web Traffic

By default, Palo Alto firewalls only log web traffic that is blocked by URL filtering policies. If you must log permitted web traffic, follow these steps.

1. In the **Objects** tab, go to **Security Profiles > URL Filtering**.
2. **Edit** an existing profile by clicking on its name, or click **Add** to create a new one.
3. For website categories that you want to log, select **Alert**.
   Traffic matching these website category definitions will be logged.
4. Click **OK**.
5. For each security rule that you want to send logs to FortiSIEM, edit the rule and add the new url filter.

Sample Parsed Palo Alto Syslog Message

```
<14>May  6 15:51:04 1,2010/05/06 15:51:04,0006C101167,TRAFFIC,start,1,2010/05/06
15:50:58,192.168.28.21,172.16.255.78,::172.16.255.78,172.16.255.78,rule3,,,icmp,vsys1,untrus
t,untrust,ethernet1/1,ethernet1/1,syslog-172.16.20.152,2010/05/06
15:51:04,600,2,0,0,0,0,0x40,icmp,allow,196,196,196,2,2010/05/06 15:50:58,0,any,0

<14>May  6 15:51:15 1,2010/05/06 15:51:15,0006C101167,SYSTEM,general,0,2010/05/06
15:51:15,,unknown,,0,0,general,informational,User admin logged in via CLI from 192.168.28.21

<14>May  9 17:55:21 1,2010/05/09 17:55:21,0006C101167,THREAT,url,6,2010/05/09
17:55:20,172.16.2.2,216.163.137.68,::172.16.255.78,216.163.137.68,DynamicDefault,,,web-
browsing,vsys1,trust,untrust,ethernet1/2,ethernet1/1,syslog-172.16.20.152,2010/05/09
17:55:21,976,1,1126,80,38931,80,0x40,tcp,block-url,"www.playboy.com/favicon.ico",
(9999),adult-and-pornography,informational,0
```

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Sophos UTM

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Configuration change, command execution	Log Management, Compliance and SIEM

Event Types

In **ADMIN > Device Support > Event Types**, search for "sophos-utm" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

Sample Syslog Message

```
<30>2016:07:05-16:57:39 c-server-1 httpproxy[15760]: id="0001" severity="info"
sys="SecureWeb" sub="http" name="http access" action="pass" method="GET" srcip="10.10.10.10"
dstip="1.1.1.1" user="" group="" ad_domain="" statuscode="302" cached="0" profile="REF_
DefaultHTTPProfile (Default Web Filter Profile)" filteraction="REF_HttCffCustoConteFilte
(Custom_Default content filter action)" size="0" request="0xdc871600" url="http://a.com"
referer="http://foo.com/bar/" error="" authtime="0" dnstime="1" cattime="24080"
avscantime="0" fullreqtime="52627" device="0" auth="0" ua="Mozilla/5.0 (Windows NT 6.1;
WOW64; Trident/7.0; rv:11.0) like Gecko" exceptions="" category="154"
reputation="unverified" categoryname="Web Ads"
```

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Sophos UTM
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Stormshield Network Security

- Integration Points
- Event Types
- Configuration
- Sample Logs

Integration Points

Protocol	Information Collected	Used For
Syslog	Firewall logs	Security and Compliance Monitoring

Event Types

Go to **RESOURCES > Event Type** and search "Stormshield-" in the main content panel **Search...** field to see the event types associated with this device.

Configuration

- Configuring Stormshield to Send Logs
- Configuring FortiSIEM to Receive Logs

Configuring Stormshield to Send Logs

Follow the steps listed here under the **Choose where to save logs** section, to save logs.

Configuring FortiSIEM to Receive Logs

No configuration is needed. FortiSIEM can automatically detect and parse Stormshield logs based on the built in parser.

Sample Logs

```
id=firewall time="2019-02-24 16:38:01" fw="SN310A17B0323A7" tz=+0100 startime="2019-02-
24 16:38:00" pri=5 confid=00 slotlevel=2 ruleid=4 rulename="1690fb96019_7"
srcif="Ethernet0" srcifname="out" ipproto=udp proto=ssdp src=10.11.11.11 srcport=49907
srcportname=ephemeral_fw_udp srcname=skywalker srcmac=11:11:11:11:11:11 dst=10.10.10.10
dstport=1900 dstportname=sdp ipv=4 sent=0 rcvd=0 duration=0.00 action=pass
logtype="filter"
```

Tigera Calico

- Integration Points
- Event Types
- Configuration
- Sample Logs

Integration Points

Protocol	Information Collected	Used For
Syslog	Flow, Audit and DNS logs	Security and Compliance Monitoring

Event Types

Go to **RESOURCES > Event Type** and search "Calico_Enterprise_" in the main content panel **Search...** field to see the event types associated with this device.

Configuration

- Configuring Tigera Calico to Send Logs
- Configuring FortiSIEM to Receive Logs

Configuring Tigera Calico to Send Logs

Follow the steps listed here to send syslog to FortiSIEM.

Configuring FortiSIEM to Receive Logs

No configuration is needed. FortiSIEM can automatically detect and parse Tigera Calico logs based on the built in parser.

Sample Logs

```
<14>May 8 15:49:58 ip-10-0-0-193.ec2.internal tigera_secure: {"start_
time":1588952982,"end_time":1588952992,"source_ip":"10.48.98.2","source_name":"elastic-
operator-0","source_name_aggr":"elastic-operator-*","source_namespace":"tigera-eck-
operator","source_port":null,"source_type":"wep","source_labels":{"labels":["k8s-
app=elastic-operator","statefulset.kubernetes.io/pod-name=elastic-operator-0","control-
plane=elastic-operator","controller-revision-hash=elastic-operator-6fc7545df5"]},"dest_
ip":"10.48.241.198","dest_name":"tigera-secure-es-es-0","dest_name_aggr":"tigera-
secure-es-es-*","dest_namespace":"tigera-elasticsearch","dest_port":9200,"dest_
type":"wep","dest_labels":{"labels":["statefulset.kubernetes.io/pod-name=tigera-secure-
es-es-0","elasticsearch.k8s.elastic.co/version=7.3.2","controller-revision-hash=tigera-
secure-es-es-757895bb98","elasticsearch.k8s.elastic.co/http-
scheme=https","elasticsearch.k8s.elastic.co/statefulset-name=tigera-secure-es-
es","elasticsearch.k8s.elastic.co/node-data=true","elasticsearch.k8s.elastic.co/config-
hash=1585026949","elasticsearch.k8s.elastic.co/node-
ml=true","common.k8s.elastic.co/type=elasticsearch","elasticsearch.k8s.elastic.co/node-
ingest=true","elasticsearch.k8s.elastic.co/node-
master=true","elasticsearch.k8s.elastic.co/cluster-name=tigera-
secure"]},"proto":"tcp","action":"allow","reporter":"dst","policies":{"all_policies":
["0|allow-tigera|tigera-elasticsearch/allow-tigera.elasticsearch-
access|allow"]},"bytes_in":2593,"bytes_out":4617,"num_flows":3,"num_flows_
started":1,"num_flows_completed":1,"packets_in":17,"packets_out":10,"http_requests_
allowed_in":0,"http_requests_denied_in":0,"original_source_ips":null,"num_original_
source_ips":0,"host":"fluentd-node-xzscj"}
```

UserGate UTM Firewall

FortiSIEM Support added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: UserGate

Product: UTM Firewall

Product Information: https://www.usergate.com/products/enterprise-firewall

- Log Information
- Event Types
- Rules
- Reports

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for usergate" to see the event types associated with this device. In FortiSIEM 6.3.1, there are 7 event types defined.

Rules

In **RESOURCES > Rules**, search for "usergate" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there is 1 rule available.

- UserGate UTM IDPS Alert Detected

Reports

In **RESOURCES > Reports**, search for "usergate" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 reports available.

- UserGate UTM - IDPS Events
- UserGate UTM - Web Access Logs

WatchGuard Firebox Firewall

- Integration Points
- Configuring Watchguard Firebox for SNMP Access
- Configuring FortiSIEM

Integration Points

Protocol	Information Discovered	Used For
SNMP	Performance metrics – CPU, Memory, Uptime, Interface Usage statistics, Connection rate and Policy Statistics	Performance and Availability Monitoring

Configuring Watchguard Firebox for SNMP Access

1. Logon to Watchguard Firebox Management Console.
2. Follow Watchguard Firebox documentation to allow inbound SNMP access (default UDP port 161) to appropriate FortiSIEM node that will communicate to Firebox node.
3. Note the SNMP credentials. FortiSIEM supports versions 1, 2 and 3.

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access:

- Define WatchGuard Firebox Firewall Credential in FortiSIEM
- Create IP Range to Credential Association, Test Connectivity, and Monitor Performance

Define WatchGuard Firebox Firewall Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Generic
Access Protocol	"SNMP" or "SNMP v3"
Port	Choose the SNMP port (default 161)

Settings	Description
Password config	**Manual** or **CyberArk**. See Password Configuration.
Community String	If "SNMP" was selected for Access Protocol, enter the community string.
Security Level/Security Name/Auth Protocol/Auth Password/Priv Protocol/Priv Password/Context	If "SNMP v3" was selected for Access Protocol, enter the detailed SNMP V3 security configuration and credentials.
Description	Description of the device.

Create IP Range to Credential Association, Test Connectivity, and Monitor Performance

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter the **IP** or **IP Range** containing the Firebox firewall in the **IP/Host Name** field. Allowed formats are comma separated IP, IP Range formatted as IP1-IP2 or IP range in CIDR notation.
   b. Select the name of the credential created in step 2 of Define WatchGuard Firebox Firewall Credential in FortiSIEM from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results. If it succeeds, your credentials are correct.
3. Go to **ADMIN > Setup > Discovery**.
4. Click **New** and create a discovery entry containing the IP Address of the Firebox firewall.
5. Click **Save**.
6. With the entry selected, click **Discover**. Ensure that the device is discovered.
7. When successful, an entry will be created in **ADMIN > Setup > Monitor Performance** corresponding to this firewall. FortiSIEM will start to pull SNMP metrics from this firewall.

Load Balancers and Application Firewalls

FortiSIEM supports these load balancers and application firewalls for discovery and monitoring.

- Barracuda Web Application Firewall
- Brocade ServerIron ADX
- Citrix Netscaler Application Delivery Controller (ADC)
- F5 Networks Application Security Manager
- F5 Networks Local Traffic Manager
- F5 Networks Web Accelerator
- Fortinet FortiADC
- Qualys Web Application Firewall

Barracuda Web Application Firewall

FortiSIEM Support added: 6.3.2

Vendor: Barracuda

Product Information: https://www.barracuda.com/products/webapplicationfirewall

- What is Discovered and Monitored
- Configuration
- Sample Events

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of Barracuda Web Application Firewall (WAF).

Protocol	Metrics Collected	Used For
Syslog	System logs, Web Firewall logs, Access logs, Audit logs and Network Firewall logs	Security and Compliance

Configuration

To configure syslog from your Barracuda WAF, take the following steps:

1. Navigate to **Advanced > Export Logs > Syslog**.
2. Configure the following fields in the table.

Field	Description
Name	Enter the name of the syslog server.
Syslog Server	Enter the IP address of the syslog server.
Log Time Stamp	Select "Yes" to log the date and time of system events.
Lot Unit Name	Select "Yes" to log the name of the Barracuda Web Application Firewall unit. The unit name is the same as the Default Host name located on the **BASIC > IP Configuration** page.
Comment	Enter any comments about the syslog server.
Select appropriate facility	Leave as Local7 or default option.

3. When done, click **Add** to add the settings.

Sample Events

```
<134>Sep 1 13:10:09 nlb_lab 2021-09-01 13:10:09.163 -0600 nlb_lab NF INFO TCP 192.0.2.105
443 ALLOW traffic:allow
<132>Sep 1 13:10:09 nlb_lab 2021-09-01 13:10:09.550 -0600 nlb_lab WF WARN UNRECOGNIZED_
COOKIE 98.98.98.22 51415 192.0.2.110 443 global GLOBAL LOG NONE [Cookie\="_derived_epik"
Service-created\="1565 days back" Reason\="No valid encrypted pair"] GET
test.example.com/random_page TLSv1.2 "-" "Mozilla/5.0 (Linux; Android 11; SAMSUNG SM-G991U)
AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/15.0 Chrome/90.0.4430.210 Mobile
Safari/537.36" 98.98.98.22 51415 "-" https://test.example.com/
<134>Sep 1 13:10:11 nlb_lab 2021-09-01 13:10:11.342 -0600 nlb_lab TR 192.0.2.105 443
192.0.2.134 53619 "-" "-" POST TLSv1.2 test.example.com HTTP/1.1 200 736974 439 0 104
10.20.20.102 443 103 "-" SERVER DEFAULT PASSIVE VALID
/json/reply/TicketingEventsGetAvailableByEventTypeName "-" "-" "-" "ServiceStack .NET Client
5.40" 192.0.2.134 53619 "-" "-" "-" "-"
```

Brocade ServerIron ADX

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
SNMP	Host name, serial number, hardware (CPU, memory, network interface etc)	Uptime, CPU, Memory, Interface Utilization, Hardware status, Real Server Statistics	Performance/Availability Monitoring

Event Types

- PH_DEV_MON_SYS_CPU_UTIL

```
[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,
[fileName]=deviceBrocadeServerIron.cpp,[lineNumber]=434,[cpuName]=CPU,[hostName]=lb1-
1008-qts,[hostIpAddr]=10.120.3.15,[cpuUtil]=55.000000,[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_SYS_MEM_UTIL

```
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,
[fileName]=deviceBrocadeServerIron.cpp,[lineNumber]=456,[memName]=Physical
Memory,[hostName]=lb1-1008-qts,[hostIpAddr]=10.120.3.15,[memUtil]=10.000000,
[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_NET_INTF_UTIL

```
[PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phIntfFilter.cpp,
[lineNumber]=323,[intfName]=GigabitEthernet8,[intfAlias]=,[hostName]=lb1-1008-qts,
[hostIpAddr]=10.120.3.15,[pollIntv]=56,[recvBytes64]=1000000,
[recvBitsPerSec]=142857.142857,[inIntfUtil]=0.014286,[sentBytes64]=2000000,
[sentBitsPerSec]=285714.285714,[outIntfUtil]=0.028571,[recvPkts64]=0,[sentPkts64]=0,
[inIntfPktErr]=0,[inIntfPktErrPct]=0.000000,[outIntfPktErr]=0,
[outIntfPktErrPct]=0.000000,[inIntfPktDiscarded]=0,[inIntfPktDiscardedPct]=0.000000,
[outIntfPktDiscarded]=0,[outIntfPktDiscardedPct]=0.000000,[outQLen64]=0,
[intfInSpeed64]=1000000000,[intfOutSpeed64]=1000000000,[intfAdminStatus]=up,
[intfOperStatus]=up,[daysSinceLastUse]=0,[totIntfPktErr]=0,
[totBitsPerSec]=428571.428571,[phLogDetail]=
```

- PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT

  ```
   [PH_DEV_MON_SERVERIRON_REAL_SERVER_STAT]:[eventSeverity]=PHL_INFO,
  [fileName]=deviceBrocadeServerIron.cpp,[lineNumber]=507,[hostName]=lb1-1008-qts,
  [hostIpAddr]=10.120.3.15,[realServerIpAddr]=10.120.10.131,[realServerState]=7,
  [failedPortExists]=2,[openConnectionsCount]=2,[peakConns]=114,[activeSessions]=4,
  [phLogDetail]=
  ```

- PH_DEV_MON_HW_STATUS

  ```
  [PH_DEV_MON_HW_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=deviceBrocadeServerIron.cpp,
  [lineNumber]=359,[hostName]=lb1-1008-qts,[hostIpAddr]=10.120.3.15,[hwStatusCode]=2,
  [hwPowerSupplyStatus]=0,[hwTempSensorStatus]=2,[hwFanStatus]=0,[phLogDetail]=

  [PH_DEV_MON_HW_STATUS_TEMP_CRIT]:[eventSeverity]=PHL_CRITICAL,[fileName]=device.cpp,
  [lineNumber]=13812,[hostName]=lb1-1008-qts,[hostIpAddr]=10.120.3.15,[hwStatusCode]=2,
  [hwComponentName]=1-Temperature
  sensor,[hwComponentStatus]=Critical,[phLogDetail]=
  ```

- PH_DEV_MON_HW_TEMP

  ```
   [PH_DEV_MON_HW_TEMP]:[eventSeverity]=PHL_INFO,[fileName]=deviceBrocadeServerIron.cpp,
  [lineNumber]=401,[hostName]=lb1-1008-qts,[hostIpAddr]=10.120.3.15,
  [hwComponentName]=Temp1,[envTempDegF]=90,[phLogDetail]=
  ```

Rules

There are no predefined rules for this device other than covered by generic network devices.

Reports

There are no predefined reports for this device other than covered by generic network devices.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Brocade ServerIron ADX
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Citrix Netscaler Application Delivery Controller (ADC)

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Example Syslog
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted and Denied traffic	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "netscaler" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "netscaler" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog

```
<182> 07/25/2012:19:56:41   PPE-0 : UI CMD_EXECUTED 473128 :  User nsroot - Remote_ip
10.13.8.75 - Command "show ns hostName" - Status "Success"<181> 07/25/2012:19:56:05  NS2-
MAIL PPE-0 : EVENT DEVICEUP 33376 :  Device "server_vip_NSSVC_SSL_172.17.102.108:443
(accellion:443)" - State UP
<181> 07/25/2012:19:55:35  NS2-MAIL PPE-0 : EVENT DEVICEDOWN 33374 :  Device "server_vip_
NSSVC_SSL_172.17.102.108:443(accellion:443)" - State DOWN
<182> 07/24/2012:15:37:08   PPE-0 : EVENT MONITORDOWN 472795 :  Monitor Monitor_http_of_
Domapps:80(10.50.15.14:80) - State DOWN
```

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Citrix NetScalar
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

F5 Networks Application Security Manager

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Various application level attack scenarios - invalid directory access, SQL injections, cross site exploits.	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "f5-asm" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog

```
<134>Jun 26 14:18:56 f5virtual.tdic.ae ASM:CEF:0|F5|ASM|10.2.1|Successful Request|Successful
Request|2|dvchost=f5virtual.adic.com dvc=192.168.1.151 cs1=master-key_default
cs1Label=policy_name cs2=master-key cs2Label=web_application_name deviceCustomDate1=Jul 13
2011 16:24:25 deviceCustomDate1Label=policy_apply_date externalId=3601068286554428885
act=passed cn1=404 cn1Label=response_code src=10.10.77.54 spt=49399 dst=10.10.175.82 dpt=443
requestMethod=POST app=HTTPS request=/ipp/port1 cs5=N/A cs5Label=x_forwarded_for_header_
value rt=Jun 26 2012 14:18:55 deviceExternalId=0 cs4=N/A cs4Label=attack_type cs6=N/A
cs6Label=geo_location cs3Label=full_request cs3=POST /ipp/port1 HTTP/1.1\r\nHost:
127.0.0.1:631\r\nCache-Control: no-cache\r\nContent-Type: application/ipp\r\nAccept:
application/ipp\r\nUser-Agent: Hewlett-Packard IPP\r\nContent-Length: 9\r\n\r\n
```

F5 Networks Local Traffic Manager

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
SNMP	Host name, serial number, hardware (CPU, memory, network interface, disk etc) and software information (running and installed software)	Uptime, CPU, Memory, Disk utilization, Interface Utilization, Hardware status, process level CPU and memory urilization	Performance/Availability Monitoring
SNMP Trap		Exception situations including hardware failures, certain security attacks, Policy violations etc	Performance/Availability Monitoring
Syslog		Permitted and Denied traffic	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "f5-LTM" to see the event types associated with this device.

Search for "f5-BigIP" in **ADMIN > Device Support > Event Types** to see event types associated with SNMP traps for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- SNMP Trap
- Example SNMP Trap
- Syslog
- Example Syslog

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example SNMP Trap

```
2012-01-18 14:13:43 0.0.0.0(via UDP: [192.168.20.243]:161) TRAP2, SNMP v2c, community public
               . Cold Start Trap (0) Uptime: 0:00:00.00         DISMAN-EVENT-
MIB::sysUpTimeInstance = Timeticks: (33131) 0:05:31.31                SNMPv2-
MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.3375.2.5.0.1
```

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog

```
<133>Oct 20 13:52:46 local/tmm notice tmm[5293]: 01200004:5: Packet rejected remote IP
172.16.128.26 port 137 local IP 172.16.128.255 port 137 proto UDP: Port closed.

<134>Jul 30 15:28:33 tmm1 info tmm1[7562]: 01070417: 134: ICSA: non-session UDP packet
accepted, source: 112.120.125.48 port: 10144, destination: 116.58.240.252 port: 53

<134>Jul 30 15:28:33 tmm1 info tmm1[7562]: 01070417: 134: ICSA: non-session TCP packet
accepted, source: 108.83.156.153 port: 59773, destination: 116.58.240.225 port: 80
```

```
<134>Jul 30 15:28:33 tmm2 info tmm2[7563]: 01070417: 134: ICSA: non-session ICMP packet
accepted, source: 10.11.218.10, destination: 10.255.111.2, type code: Echo Reply
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

F5 Networks Web Accelerator

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted traffic	Log analysis and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "f5-web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog

```
<182>Oct 20 13:52:56 local/BadReligion1 info logger: [ssl_acc] 1.1.1.2 - admin [20/Oct/2011:
13:52:56 -0400] "POST /iControl/iControlPortal.cgi HTTP/1.1" 200 654
```

Fortinet FortiADC

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
syslog	Host name, Reporting IP	None	Event, Security and Traffic logs	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiADC" to see the event types associated with this device.

Rules

No specific rules are written for FortiADC Web application firewall but generic firewall rules will apply.

Reports

No specific reports are written for FortiADC Web application firewall but generic firewall rules will apply.

Configuration

Configure FortiADC Web application firewall to send logs to FortiSIEM in the supported format (see Sample Events).

To configure a syslog object in FortiADC, take the following steps:

Note: Refer to the FortiADC Handbook for the most recent configuration information. Configuration taken from 6.1.2 FortiADC Handbook.

1. Go to **System > Alert > Alert Resource** and select the **Syslog** tab.
2. Click **Create New**.

3. Complete the configuration as described in the following table.

Settings	Guidelines
Name	Enter a name for the syslog message object. No spaces. You will use this name to select the syslog in an Alert Actions profile.
Syslog Server	Enter the IP address of the syslog server that will receive syslog messages.
Port	Enter the port of the syslog server. The default is 514.

4. Click **Save**.

Settings for Access Credentials

None required

Sample Events

```
<6>date=2019-06-12 time=13:05:52 device_id=FAD2KD3114000026 log_id=0000000100 type=event
subtype=config pri=information vd=root msg_id=71118385 user=user1 ui=GUI(1.2.3.4) action=add
cfgpath=log setting remote cfgobj=<No.> cfgattr=1 logdesc=Change the configuration
msg="added a new entry '1' for "log setting remote" on domain "root””
```

```
<1>date=2019-06-12 time=13:06:52 device_id=FAD2KD3114000026 log_id=0003000235 type=event
subtype=system pri=alert vd=root msg_id=71118386 submod=update user=system ui=system
action=update status=none logdesc=License could not be validated msg="Unable to connect to
FDS server"
```

Qualys Web Application Firewall

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted and Denied Web traffic	Log analysis and compliance

Event Types

The following event types are generated by parsing Qualys Web Application Firewall traffic logs and analyzing the HTTP error code.

- Qualys-WAF-Web-Request-Success
- Qualys-WAF-Web-Bad-Request
- Qualys-WAF-Web-Client-Access-Denied
- Qualys-WAF-Web-Client-Error
- Qualys-WAF-Web-Forbidden-Access-Denied
- Qualys-WAF-Web-Length-Reqd-Access-Denied
- Qualys-WAF-Web-Request
- Qualys-WAF-Web-Request-Redirect
- Qualys-WAF-Web-Server-Error

Rules

There are no predefined rules for this device.

Reports

Relevant reports are defined in **RESOURCES > Reports > Device > Network > Web Gateway**.

Configuration

FortiSIEM processes events from this device via syslog sent in **JSON format**. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Qualys Web Application Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

Note that each JSON formatted syslog contains many logs.

```
<1350>1 2015-05-15T12:57:30.945000+00:00 localhost qualys_waf - QUALYS_WAF -
{"timestamp":"2015-05-15T12:57:30.945-00:00","duration":6011,"id":"487c116c-4908-4ce3-b05c-
eda5d5bb7045","clientIp":"172.27.80.170","clientPort":9073,"sensorId":"d3acc41f-d1fc-43be-
af71-e7e10e9e66e2","siteId":"41db0970-8413-4648-b7e2-c50ed53cf355","connection":
{"id":"bc1379fe-317e-4bae-ae30-
2a382e310170","clientIp":"172.27.80.170","clientPort":9073,"serverIp":"192.168.60.203","serv
erPort"
```

```
:443},"request":{"method":"POST","uri":"/","protocol":"HTTP/1.1","host":"esers-
test.foo.org","bandwidth":0,"headers":[{"name":"Content-Length","value":"645"},
{"name":"Accept","value":"text/html,application/xhtml+xml,application/xml;q=0.9,image/web
p,*/*;
```

```
q=0.8"},{"name":"User-Agent","value":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36"},{"name":"Content-
Type","value":"application/x-www-form-urlencoded"},{"name":"Referer","value":"https://esers-
test.ohsers.org/"},{"name":"Accept-Encoding","value":"gzip, deflate"},{"name":"Accept-
Language","value":"en-US,en;q=0.8"}],"headerOrder":"HILCAUTRELO"},"response":
{"protocol":"HTTP/1.1","status":"200","message":"OK","bandwidth":0,"headers":
[{"name":"Content-Type","value":"text/html; charset=utf-8"},
{"name":"Server","value":"Microsoft-IIS/8.5"},{"name":"Content-
Length","value":"10735"}],"headerOrder":"CTXSDL"},"security":{"auditLogRef":"b02f96e9-2649-
4a83-9459-6a02da1a5f05","threatLevel":60,"events":[{"tags":
["qid/226015","cat/XPATHi","cat/SQLi","qid/150003","loc/req/body/txtUserId","cfg/pol/applica
tionSecurity"],
"type":"Alert","rule":"main/qrs/sqli/xpathi/condition_escaping/boolean/confidence_
high/3","message":"Condition escaping detected (SQL or XPATH injection) -
txtUserId.","confidence":80,"severity":60,"id":"262845566"},{"tags":
["cat/correlation","qid/226016"],"type":"Observation","rule":"main/correlation/1",

"message":"Info: Threat level exceeded blocking threshold
(60).","confidence":0,"severity":0,"id":"262846018"},{"tags":
["cat/correlation","qid/226016"],"type":"Observation","rule":"main/correlation/1",

"message":"Info: Blocking refused as blocking mode is
disabled.","confidence":0,"severity":0,"id":"262846167"},{"tags":
["cat/correlation","cat/XPATHi","qid/226015"],"type":"Alert","rule":

"main/correlation/1","message":"Detected:
XPATHi.","confidence":80,"severity":60,"id":"268789851"}]}}
```

Log Aggregators

FortiSIEM supports these devices.

- FortiAnalyzer

Fortinet FortiAnalyzer

- Overview
- Configuring FortiAnalyzer
- Configuring FortiSIEM Collectors to Receive Logs from FortiAnalyzer
- Configuring FortiAnalyzer to Forward its own System Event Logs

Overview

Customers of both FortiAnalyzer and FortiSIEM may want to take already aggregated event data received on FortiAnalzyer and forward those events to FortiSIEM.

Configuring FortiAnalyzer

- Setting Up the Syslog Server
- Pre-Configuration for Log Forwarding
- Configuring Log Forwarding

Setting Up the Syslog Server

1. Login to FortiAnalyzer.
2. Go to **System Settings** > **Advanced** > **Syslog Server**.
   a. Click the **Create New** button.
   b. Enter the **Name**. (It is recommended to use the name of the FortiSIEM server.)
   c. Fill in the **IP address** (or **FQDN**) with the IP or a fully qualified name of the FortiSIEM server.
   d. Leave the **Syslog Server Port** to the default value '514'.
   e. Click **OK** to save your entries.

Pre-Configuration for Log Forwarding

To configure FortiAnalyzer event forwarding to FortiSIEM, you must first set up the following.

1. Install a FortiSIEM collector in the same subnet as FortiAnalyzer that will be forwarding the events.
   Note: The same subnet request is required as FortiAnalyzer will later be configured to spoof packets to the collector. RPF (reverse path forwarding checks) on network equipment would have to be disabled if FortiAnalyzer and collector existed on different subnets.

2. It is recommended that for every 5,000 EPS (events per second) ingested, you add 1 collector that is 8vCPU, 8GB RAM. If you have more than 5,000 EPS forwarding from FortiAnalyzer, please set up a load balancer with multiple collectors behind it, allowing UDP 514 inbound.

Configuring Log Forwarding

Take the following steps to configure log forwarding on FortiAnalyzer.

1. Go to **System Settings > Log Forwarding**.
2. Click the **Create New** button in the toolbar. The **Create New Log Forwarding** pane opens.
3. fill in the information as per the below table, then click **OK** to create the new log forwarding. The FortiAnalyzer device will start forwarding logs to the server.

Field	Input
Name	FortiSIEM-Forwarding
Status	On
Remote Server Type	Syslog
Compression	OFF
Sending Frequency	Real-time
Log Forwarding Filters	Select all desired Administrative Domains (ADOMs) / device logs you'd like to forward

4. Go to the CLI Console and configure the CLI only log forward option by running the following CLI commands.
   Notes:
   - Logs received by FortiAnalyzer, and then forwarded to FortiSIEM, have the source IP of the log packet overwritten with the IP address of the FortiAnalyzer appliance. This hides the “true” source of the log packet from FortiSIEM. To override this behavior, FortiAnalyzer can spoof the original log sender's IP address when forwarding to FortiSIEM. This allows FortiSIEM collectors to receive all the original information as if it received the logs directly from the originating device.
   - For FortiAnalyzer versions 6.0 and later, use the following CLI:

     Note: Replace <*id*> with the actual name of the log forward created earlier.

     ```
     config system log-forward
         edit <id>
             set mode forwarding
             set fwd-max-delay realtime
             set server-name "<FSM_Collector>"
             set server-ip "a.b.c.d"
             set fwd-log-source-ip original_ip
             set fwd-server-type syslog
         next
     end
     ```

   - For FortiAnalyzer versions 5.6 to 5.9, use the following CLI:
     Note: Replace <*id*> with the actual name of the log forward created earlier.

     ```
     config system log-forward

       edit <id>
     ```

```
      set mode forwarding
      set fwd-max-delay realtime
      set server-ip "a.b.c.d"
      set fwd-log-source-ip original_ip
      set fwd-server-type syslog
  next
end
```

- For FortiAnalyzer versions earlier than 5.6, use the following CLI:
  Note: Replace <*id*> with the number for your FortiSIEM syslog entry.

```
config system aggregation-client
  edit <id>
    set fwd-log-source-ip original_ip
end
```

- To configure FortiAnalyzer to forward its own local logs, see Configuring FortiAnalyzer to Forward its own System Event Logs.

Configuring FortiSIEM Collector to Receive Logs from FortiAnalyzer

To configure the FortiSIEM collector to receive logs from FortiAnalyzer, you will need to disable RPF checks that would normally cause the collector virtual machine from dropping the log packet as it is spoofed.

```
sysctl -w net.ipv4.conf.all.rp_filter=0
```

To make this change persistent across reboots, add the following code to the `/etc/sysctl.conf` file.

```
net.ipv4.conf.all.rp_filter=0
```

Configuring FortiAnalyzer to Forward its own System Event Logs

FortiAnalyzer can forward two primary types of logs, each configured differently:

- Events received from other devices (FortiGates, FortiMail, FortiManager, etc)
- Locally generated System events (FortiAnalyzer admin login attempts, config changes, etc)

FortiAnalyzer System Event Logs via Syslog

- 9 event types
- no rules
- no reports
- no dashboards

Configuring FortiAnalyzer System's Local Log

To configure the system's local log, replace the IP with the IP of the FortiSIEM collector.

```
config system syslog
edit "fortisiem"
                set ip "192.168.1.1"
end
config system locallog syslogd setting
set status enable
set syslog-name "fortisiem"
end
```

Network Compliance Management Applications

FortiSIEM supports these Network Compliance Management applications and monitoring.

- Cisco Network Compliance Manager
- PacketFence

Cisco Network Compliance Manager

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Example Syslog

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Network device software update, configuration analysis for compliance, admin login	Log analysis and compliance

Event Types

Over 40 event types are generated by parsing Cisco Network Configuration Manager logs. The complete list can be found in **ADMIN > Device Support > Event Types** by searching for "Cisco-NCM". Some important ones are

- Cisco-NCM-Device-Software-Change
- Cisco-NCM-Software-Update-Succeeded
- Cisco-NCM-Software-Update-Failed
- Cisco-NCM-Policy-Non-Compliance
- Cisco-NCM-Device-Configuration-Deployment
- Cisco-NCM-Device-Configuration-Deployment-Failure

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Example Syslog

Note that each JSON formatted syslog contains many logs.

```
490998571 Mon Mar 03 03:09:31 EST 2014 Savvy Device Command Script Completed Successfully
server01.foo.com 10.4.161.32 Script 'Re-enable EasyTech port for Cisco IOS configuration'
completed.  Connect - Succeeded Connected via ssh to 10.170.30.9 [in realm Default Realm]
Login / Authentication - Succeeded Successfully used: Last successful password  (Password
rule Retail TACACS NCM Login)    Optional:Script - Succeeded Successfully executed: prepare
configuration for deployment  Script - Succeeded Successfully executed: deploy to running
configuration via TFTP through CLI Bypassed: deploy to running configuration via SCP through
CLI.  (Requires SCP, CLI to be enabled.) Tried: deploy to running configuration via FTP
through CLI (Warning: SSH server username or password not specified in NA admin settings.)
Optional:Script - Succeeded Successfully executed: determine result of deployment operation
Script run: ------------------------------------------------------------ ! interface
fast0/16 no shut

491354611 Tue Mar 04 03:38:22 EST 2014 FooA Software Update Succeeded server01.foo.com
1.1.1.32  44571 10.173.30.9 $OrignatorEmail$ FooA Update Device Software 2014-03-04
03:30:00.0 usmist_1699295009 (1.13.3.9) Succeeded
```

PacketFence Network Access Control (NAC)

- Integration Points
- Event Types
- Configuring PacketFence Network Access Control

Integration Points

Protocol	Information Discovered	Used For
Syslog	User network admission control events	Security and Compliance

Event Types

Over 20 events are parsed. See event types in **RESOURCES > Event Types** and search for "PacketFence-NAC-" in the main content panel **Search...** field.

Configuring PacketFence NAC

Follow PacketFence NAC documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes PacketFence NAC syslog as long as it follows the format shown in the sample syslog:

```
Oct 9 11:29:34 10.2.204.81 1 2018-10-09T11:29:34.04189+01:00 example.com packetfence.log - -
- Oct 11 15:42:00 httpd.aaa(4765) WARN: [mac:40:83:1d:12:2a:cb] Calling match with
empty/invalid rule class. Defaulting to 'authentication' (pf::authentication::match)
```

Network Intrusion Detection System

FortiSIEM supports these devices.

- Microsoft Advanced Threat Analytics (ATA) On Premise Platform
- Zeek Network Security Monitor (Previously known as Bro)

Microsoft Advanced Threat Analytics (ATA) On Premise Platform

FortiSIEM Support added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Microsoft

Product Information: https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata

Microsoft Advanced Threat Analytics (ATA) is an on-premises platform that helps protect enterprises from multiple types of advanced targeted cyber attacks and insider threats.

- Log Information
- Event Types
- Rules
- Reports

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "microsoft-ata" to see the event types associated with this device.

In 6.3.1, there are 51 event types.

Rules

In **RESOURCES > Rules**, search for "microsoft ata" in the main content panel **Search...** field to see related rules associated with this device.

In FortiSIEM 6.3.1, there is 1 rule available.

- Microsoft ATA Center: Security Alert Triggered

Reports

In **RESOURCES > Reports**, search for "microsoft ata" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 reports available.

- Microsoft ATA (Advanced Threat Analytics) Center - Change Audit Events
- Microsoft ATA (Advanced Threat Analytics) Center - Security Alerts

Zeek Network Security Monitor (Previously known as Bro)

FortiSIEM Support added: 5.2.5 (Installed on Security Onion)

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Zeek

Product Information: https://zeek.org/

- Log Information
- Event Types
- Rules
- Reports
- Configuration

Log Information

Log Collection Method	Log Body Format Accepted	Purpose
Syslog (via Rsyslog)	JSON	Security and Compliance

Event Types

In 6.3.1, there are 29 event types.

Rules

There are no specific rules for Zeek Network Security Monitor.

Reports

There are no specific reports for Zeek Network Security Monitor.

Configuration

To forward logs to FortiSIEM, they must be configured to follow a specific format. Prior to this configuration, you may need to configure Zeek to output logs to JSON format. If you are using Security Onion with Zeek, you can skip the Configuring Zeek to Output Logs to JSON as Security Onion by default configures Zeek for JSON.

- Configuring Zeek to Output Logs to JSON
- FortiSIEM Expected Format
- Zeek Deployment through Security Onion Rsyslog Configuration
- Standalone Zeek Deployment Rsyslog Configuration

Configuring Zeek to Output Logs to JSON

To configure Zeek to output logs to JSON, take the following steps:

1. Stop Zeek if it is running by using the following command.
   ```
   zeekctl stop
   ```
2. Edit `/opt/zeek/share/zeek/site/local.zeek` by adding the following line.
   ```
   @load policy/tuning/json-logs.zeek
   ```
3. Restart Zeek and confirm logs are stored in JSON format by running the follow commands.
   ```
   zeekctl deploy
   cd /opt/zeek/logs/current
   less conn.logs
   ```

FortiSIEM Expected Format

Rsyslog or Syslog NG configuration is required to pickup the desired logs using FortiSIEM's expected format.

```
Example Format of Log:
<190>Jun 16 17:55:50 host1 zeek_conn: {}
```

The log type is appended to `zeek_<log file name>`. See here for more information.

Rsyslog or Syslog-ng must be configured to pick up the defined log files and put them in the correct expected header format.

```
<190>Jun 16 17:55:50 host1 zeek_<log_file_name> <log body>
```

Example:

```
<190>Jun 16 17:55:50 co-nuc zeek_conn:
{"ts":1623862540.702791,"uid":"CBeSUC20TqYMeNKaL4","id.orig_h":"192.168.77.115","id.orig_
p":58734,"id.resp_h":"1.1.1.1","id.resp_p":443,"proto":"tcp","conn_state":"OTH","local_
orig":true,"local_resp":false,"missed_bytes":0,"history":"C","orig_pkts":0,"orig_ip_
bytes":0,"resp_pkts":0,"resp_ip_bytes":0}
```

This format is achieved in rsyslog if you specify an input file tag when opening the log file as shown here.

```
$InputFileTag zeek_conn:
```

Choose the configuration that matches your environment.

- Zeek Deployment through Security Onion Rsyslog Configuration
- Standard Zeek Deployment Rsyslog Configuration

Zeek Deployment through Security Onion Rsyslog Configuration

If your Zeek deployment is through Security Onion, and you are using the Centos 7 + docker ISO download, you can use rsyslog to collect the log files. The path to your logs should be here: `/nsm/zeek/logs/current`. The default format is already JSON.

Under this folder, you have several defaults, listed here:

```
broker.log
capture_loss.log
cluster.log
conn.log
loaded_scripts.log
notice.log
packet_filter.log
reporter.log
stats.log
stderr.log
stdout.log
weird.log
```

Take the following steps:

1. Open the Rsyslog file using the following command.
   ```
   vi /etc/rsyslog.conf
   ```
2. Under the Modules section, add the following line.
   $ModLoad imfile
3. In between the Global Directives and Rules sections, add the following:
   ```
   $InputFileName /nsm/zeek/logs/current/notice.log
   $InputFileTag zeek_notice:
   $InputFileStateFile stat-zeek_notice
   $InputFileSeverity info
   $InputFileFacility local7
   $InputRunFileMonitor

   $InputFileName /nsm/zeek/logs/current/cluster.log
   $InputFileTag zeek_cluster:
   $InputFileStateFile stat-zeek_cluster
   $InputFileSeverity info
   ```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/loaded_scripts.log
$InputFileTag zeek_loaded_scripts:
$InputFileStateFile stat-zeek_loaded_scripts
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/conn.log
$InputFileTag zeek_conn:
$InputFileStateFile stat-zeek_conn
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dns.log
$InputFileTag zeek_dns:
$InputFileStateFile stat-zeek_dns
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/http.log
$InputFileTag zeek_http:
$InputFileStateFile stat-zeek_http
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dhcp.log
$InputFileTag zeek_dhcp:
$InputFileStateFile stat-zeek_dhcp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ntp.log
$InputFileTag zeek_ntp:
$InputFileStateFile stat-zeek_ntp
$InputFileSeverity info
```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dce_rpc.log
$InputFileTag zeek_dce_rpc:
$InputFileStateFile stat-dce_rpc
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/kerberos.log
$InputFileTag zeek_kerberos:
$InputFileStateFile stat-kerberos
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ntlm.log
$InputFileTag zeek_ntlm:
$InputFileStateFile stat-ntlm
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ssl.log
$InputFileTag zeek_ssl:
$InputFileStateFile stat-zeek_ssl
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/files.log
$InputFileTag zeek_files:
$InputFileStateFile stat-zeek_files
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/x509.log
$InputFileTag zeek_x509:
$InputFileStateFile stat-zeek_x509
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/pe.log
$InputFileTag zeek_pe:
$InputFileStateFile stat-zeek_pe
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/rdp.log
$InputFileTag zeek_rdp:
$InputFileStateFile stat-zeek_rdp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/traceroute.log
$InputFileTag zeek_irc:
$InputFileStateFile stat-zeek_traceroute
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/dpd.log
$InputFileTag zeek_dpd:
$InputFileStateFile stat-zeek_dpd
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/software.log
$InputFileTag zeek_software:
$InputFileStateFile stat-zeek_software
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/weird.log
$InputFileTag zeek_weird:
$InputFileStateFile stat-zeek_weird
$InputFileSeverity info
```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/known_services.log
$InputFileTag zeek_known_services:
$InputFileStateFile stat-zeek_known_services
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/known_hosts.log
$InputFileTag zeek_known_hosts:
$InputFileStateFile stat-zeek_known_hosts
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/known_certs.log
$InputFileTag zeek_known_certs:
$InputFileStateFile stat-zeek_known_certs
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /nsm/zeek/logs/current/capture_loss.log
$InputFileTag zeek_capture_loss:
$InputFileStateFile stat-zeek_capture_loss
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
```

4. at the bottom of the Rules section, add the following check for new lines every second.

   ```
   $InputFilePollingInterval 1
   local7.info @<ip or FQDN of the FortiSIEM collector>
   ```

5. Save the file.
6. Restart Rsyslog by running the following command.

   ```
   systemctl restart rsyslog
   ```

As events occur for Zeek, these logs will be sent to the location specified under @<*ip or FQDN of the FortiSIEM collector*>.

Standalone Zeek Deployment Rsyslog Configuration

For standalone Zeek deployment, log file location is most typically here:

```
/opt/zeek/logs/current
```

If your log file path is neither of these, replace the following commands with your correct path.

Take the following steps:

1. Open the Rsyslog file using the following command.

   ```
   vi /etc/rsyslog.conf
   ```

2. Under the Modules section, add the following line.

```
$ModLoad imfile
```

3. In between the Global Directives and Rules sections, add the following:

```
$InputFileName /opt/zeek/logs/current/notice.log
$InputFileTag zeek_notice:
$InputFileStateFile stat-zeek_notice
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/conn.log
$InputFileTag zeek_conn:
$InputFileStateFile stat-zeek_conn
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dns.log
$InputFileTag zeek_dns:
$InputFileStateFile stat-zeek_dns
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/http.log
$InputFileTag zeek_http:
$InputFileStateFile stat-zeek_http
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dhcp.log
$InputFileTag zeek_dhcp:
$InputFileStateFile stat-zeek_dhcp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ntp.log
$InputFileTag zeek_ntp:
$InputFileStateFile stat-zeek_ntp
$InputFileSeverity info
```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dce_rpc.log
$InputFileTag zeek_dce_rpc:
$InputFileStateFile stat-dce_rpc
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/kerberos.log
$InputFileTag zeek_kerberos:
$InputFileStateFile stat-kerberos
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ntlm.log
$InputFileTag zeek_ntlm:
$InputFileStateFile stat-ntlm
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ssl.log
$InputFileTag zeek_ssl:
$InputFileStateFile stat-zeek_ssl
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/files.log
$InputFileTag zeek_files:
$InputFileStateFile stat-zeek_files
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/x509.log
$InputFileTag zeek_x509:
$InputFileStateFile stat-zeek_x509
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/smtp.log
$InputFileTag zeek_smtp:
$InputFileStateFile stat-zeek_smtp
$InputFileSeverity info
```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ssh.log
$InputFileTag zeek_ssh:
$InputFileStateFile stat-zeek_ssh
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/pe.log
$InputFileTag zeek_pe:
$InputFileStateFile stat-zeek_pe
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/ftp.log
$InputFileTag zeek_ftp:
$InputFileStateFile stat-zeek_ftp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/rdp.log
$InputFileTag zeek_rdp:
$InputFileStateFile stat-zeek_rdp
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/traceroute.log
$InputFileTag zeek_irc:
$InputFileStateFile stat-zeek_traceroute
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/dpd.log
$InputFileTag zeek_dpd:
$InputFileStateFile stat-zeek_dpd
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/software.log
$InputFileTag zeek_software:
$InputFileStateFile stat-zeek_software
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/weird.log
$InputFileTag zeek_weird:
$InputFileStateFile stat-zeek_weird
$InputFileSeverity info
```

```
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/known_services.log
$InputFileTag zeek_known_services:
$InputFileStateFile stat-zeek_known_services
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/known_hosts.log
$InputFileTag zeek_known_hosts:
$InputFileStateFile stat-zeek_known_hosts
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/known_certs.log
$InputFileTag zeek_known_certs:
$InputFileStateFile stat-zeek_known_certs
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor

$InputFileName /opt/zeek/logs/current/capture_loss.log
$InputFileTag zeek_capture_loss:
$InputFileStateFile stat-zeek_capture_loss
$InputFileSeverity info
$InputFileFacility local7
$InputRunFileMonitor
```

4. At the bottom of the Rules section, add the following check for new lines every second.

   ```
   $InputFilePollingInterval 1
   local7.info @<ip or FQDN of FortiSIEM collector>
   ```

5. Save the file.
6. Restart Rsyslog by running the following command.

   ```
   systemctl restart rsyslog
   ```

As events occur for Zeek, these logs will be sent to the location specified under @<*ip or FQDN of FortiSIEM collector*>.

Network Intrusion Prevention Systems (IPS)

FortiSIEM supports these intrusion prevention systems for discovery and monitoring.

- 3COM TippingPoint UnityOne IPS
- AirTight Networks SpectraGuard
- Alert Logic IRIS API
- Claroty Continuous Threat Detection
- Cisco Firepower Management Center (FMC) - Formerly FireSIGHT and FirePower Threat Defense
- Cisco Intrusion Prevention System
- Cisco Stealthwatch
- Corero Smartwall Threat Defense System
- Cylance Protect Endpoint Protection
- Cyphort Cortex Endpoint Protection
- Damballa Failsafe
- Darktrace CyberIntelligence Platform
- Dragos Platform
- FireEye Malware Protection System (MPS)
- FortiDDoS
- Fortinet FortiDeceptor
- Fortinet FortiNAC
- Fortinet FortiSandbox
- Fortinet FortiTester
- IBM Internet Security Series Proventia
- Indegy Security Platform
- Juniper DDoS Secure
- Juniper Networks IDP Series
- McAfee IntruShield
- McAfee Stonesoft IPS
- Motorola AirDefense
- Nozomi
- Palo Alto Cortex XDR
- Radware DefensePro
- Snort Intrusion Prevention System
- Sourcefire 3D and Defense Center
- Trend Micro Deep Discovery
- Zeek (Bro) Installed on Security Onion

3Com TippingPoint UnityOne IPS

- What is Discovered and Monitored
- Event Types
- Configuration
- Sample Parsed Syslog Messages
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP		CPU, memory, Interface utilization	Performance and Availability Monitoring
Syslog		IPS Alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "tippingpoint" to see the event types associated with this device.

Configuration

- SNMP
- Syslog

SNMP

1. Log in to the TippingPoint appliance or the SMS Console.
2. Go to **System > Configuration > SMS/NMS**.
3. For **SMS Authorized IP Address/CIDR**, make sure **any** is entered.
4. Select **Enabled** for **SNMP V2**.
5. For **NMS Community String**, enter `public`.
6. Click **Apply**.

Syslog

1. Log in to the TippingPoint appliance or the SMS Console.
2. Go to **System > Configuration > Syslog Servers**.
3. Under **System Log**, enter the **IP Address** of the FortiSIEM virtual appliance.
4. Select **Enable syslog offload for System Log**.

5. Under **Aud Log**, enter the **IP Address** of the FortiSIEM virtual appliance.
6. Select **Enable syslog offload for Audit Log**.
7. Click **Apply**.

Configure the Syslog Forwarding Policy (Filter Notification Forwarding)

The filter log can be configured to generate events related to specific traffic on network segments that must pass through the device. This log includes three categories of events.

Event Category	Description
Alert	Alert events indicate that the IPS has detected suspicious activity in the packet, but still permits the packet to pass through (specific settings are controlled by administrator profile)
Block	Block events are malicious packets not permitted to pass
P2P	Refers to peer-to-peer traffic events

In addition, filter events contain a UUID, which is a unique numerical identifier that correlates with the exact security threat defined by Tipping Point Digital Vaccine Files. The FortiSIEM Virtual Appliance will correlate these with authoritative databases of security threats.

1. Go to **IPS > Action Sets**.
2. Click **Permit + Notify**.
3. Under Contacts, click Remote Syslog.
4. Under **Remote Syslog Information**, enter the **IP Address** of the FortiSIEM virtual appliance.
5. Make sure the **Port** is set to **514**.
6. Make sure **Delimiter** is set to **tab, comma,** or **semicolon**.
7. Click **Add to Table Below**.
   You should now see the IP address of the FortiSIEM virtual appliance appear as an entry in the **Remote Syslogs** table.

Sample Parsed Syslog Messages

- Directly from TippingPoint IPS Device
- From Tipping Point NMS Device

Directly from TippingPoint IPS Device

```
<36>Oct 28 13:10:45 9.0.0.1 ALT,v4,20091028T131045+0480,"PH-QA-
      TIP1"/20.30.44.44,835197,1,Permit,Minor,00000002-0002-0002-0002-000000000089, "0089:
      IP: Short Time To Live (1)","0089: IP: Short Time To Live (1)",ip,"
      ",172.16.10.1:0,224.0.0.5:0,20091028T130945+0480,6," ",0,1A-1B <37>Nov 5 20:16:19
      20.30.44.44 BLK,v4,20091105T201619+0480,"PH-QA-
      TIP1"/20.30.44.44,70,2,Block,Low,00000002-0002-0002-0002-000000004316, "4316: OSPF:
      OSPF Packet With Time-To-Live of 1","4316: OSPF: OSPF Packet With Time-To-Live of
      1",ip," ",172.16.10.1:0,224.0.0.5:0,20091105T201619+0480,1," ",0,1A-1B <37>Jul 12
      15:04:01 SOCIPS01 ALT,v5,20110712T150401-
      0500,SOCIPS01/192.168.10.122,3225227,1,Permit,Low,00000002-0002-0002-0002-
      000000010960, "10960: IM: Google GMail Chat SSL Connection Attempt","10960: IM: Google
      GMail Chat SSL Connection Attempt",tcp," ",156.63.133.8,10948,72.14.204.189,443,
      20110712T150239-0500,3," ",0,6A-6B
```

From Tipping Point NMS Device

```
<36> 7 2 00000002-0002-0002-0002-000000001919 00000001-0001-0001-0001-000000001919 1919:
     Backdoor: Psychward 1919 tcp 10.1.1.100 13013 10.1.1.101 1240 3 3 2 207-2400-Jack
     33761793 1109876221622 <36> 7 2 00000002-0002-0002-0002-000000001919 00000001-0001-
     0001-0001-000000001919 1919: Backdoor: Psychward 1919 tcp 10.1.1.100 13013 10.1.1.101
     1240 3 3 2 207-2400-Jack 33761793 1109876221622
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	3Com TippingPoint UnityOne IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

AirTight Networks SpectraGuard

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Example Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "airtight" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Airtight SpectraGuard
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<30><2013.09.09 19:45:16>CEF:0|AirTight|SpectraGuard Enterprise|6.7|5.51.515|
Authorized AP operating on non-allowed channel|3|msg=Stop:
Authorized AP [AP2.12.c11d] is operating on non-allowed channel.
rt=Sep 09 2013 19:45:16 UTC dvc=10.255.1.36 externalId=726574
dmac=58:BF:EA:FA:26:EF cs1Label=TargetDeviceName
cs1=AP2.12.c11d cs2Label=SSID cs2=WiFiHiSpeed cs3Label=SecuritySetting
cs3=802.11i cn1Label=RSSI_dBm cn1=-50 cn2Label=Channel cn2=149
cs4Label=Locationcs4=//FB/FBFL2
```

Alert Logic IRIS API

Support for Alert Logic IRIS API allows FortiSIEM to respond to incidents and events in real-time with up-to-date situational awareness and comprehensive security analytics.

- Integration Points
- Event Types
- Rules
- Reports
- Configuring AlertLogic IRIS for FortiSIEM API Access
- Configuring FortiSIEM for AlertLogic IRIS API Access
- Sample Events

Integration Points

Protocol	Information Discovered	Used For
AlertLogic Iris API	Security Alerts created by AlertLogic	Security and Compliance

Event Types

In **RESOURCES > Event Types**, enter "AlertLogic" in the main content panel **Search...** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, enter "AlertLogic" in the main content panel **Search...** field to see the rules associated with this device.

Reports

No defined reports.

Configuring Alert Logic for FortiSIEM API Access

Get API Key from Alert Logic

1. Login to the Alert Logic user interface.
2. On the left menu, select **Admin >Account**.
3. Click **New API Key**.
4. Enter a descriptive name in the **Generate New API key** dialog box.

5. Click **Save** to generate the API key.
   A file containing your API key information (**ID**, **ClientSecret**, and **Name**) will be downloaded. The **ID** and **ClientSecret** will be used by FortiSIEM.

Configuring FortiSIEM for Alert Logic API Access

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

Settings	Description
Name	Enter a name for the credential
Device Type	Alert Logic IPS
Access Protocol	Alert Logic IPS
Pull Interval	The interval in which FortiSIEM will pull events from Alert Logic. Default is 5 minutes.
Access Key ID	Access key for your Alert Logic instance.
Secret Key	Secret key for your Alert Logic instance
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your Alert Logic credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Alert Logic.
5. To see the jobs associated with Alert Logic, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Alert Logic" in the search box.

Sample Events

Raw events of an incident start with `[AlertLogic_Incident]`:

```
[AlertLogic_Incident]:[reptDevIpAddr]=10.10.10.10,
[reptDevName]=api.cloudinsight.alertlogic.com,[accountId]=11111111.0,[phCustId]=1,
[inIncidentAcknowledgeStatus]=closed,[inIncidentEventFirstSeen]=1558710055.0,
[inIncidentClearedTime]=1558710055.0,[inIncidentCreateTime]=1558710161.9708278,
[inIncidentCreatedUserId]=,[inIncidentLastModifiedTime]=0,
[inIncidentLastModifiedUser]=,[inCustomerName]=1074822-INT4 - RMS FAWS Test,[msg]=This
is a correlation incident,[inIncidentId]=e911347e8c1ca0fa,[inIncidentStatus]=closed,
[attackType]=suspicious-activity,[type]=,[count]=0.0,[comment]=Test,[eventSeverity]=5,
[eventType]=AlertLogic-Incident-Mei_Test,[srcIpAddr]=255.255.255.255,
[destIpAddr]=255.255.255.255
```

Raw events of an associated event start with `[AlertLogic_Incident_Associated_Event]`:

```
AlertLogic_Incident_Associated_Event]:[reptDevIpAddr]=10.10.10.10,[phCustId]=,
[reptDevIpAddr]=34.192.118.124,[reptDevName]=api.cloudinsight.alertlogic.com,
[accountId]=100000,[inIncidentId]=e9113683d6815742,[httpContentType]=application/x-
alpacket-megmsgs,[description]=meta,[resourceType]=associated log,[resourceName]=Log,
[uuid]=UVUxSk5BQ2tNS3NBQUFBQVhQQnNkRnp3YkhRQUFiRE1BQUVBSG1Gd2NHeHBZMkYwYVc5dUwzZ3RZV3h3
WVdOclpYUXRiV1ZuYlhObmN3QUdURTlIVFZOSDphcHBsaWNhdGlvbi94LWFscGFja2V0LW1lZ21zZ3M6ZTkxMTM
2ODNkNjgxNTc0MjoxMDc2MDM2Mw==,[hostName]=meta,[msg]=dddddddd,[eventSeverity]=5,
[procId]=0,[procName]=meta,[collectorTime]=1559260276,[reptDevName]=user,
[eventType]=AlertLogic_e9113683d6815742_Associated_Event
```

Cisco Firepower Management Center (FMC) - Formerly FireSIGHT and FirePower Threat Defense

Cisco Firepower Management Center (FMC) provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. It can easily go from managing a firewall to controlling applications to investigating and remediating malware outbreaks.

This section describes how FortiSIEM collects logs from Cisco FireSIGHT console and FirePower Threat Defense via the eStreamer API integration. FortiSIEM provides two integrations options, either through the FortiSIEM built-in eStreamer integration or via the Cisco FirePower eStreamer eNcore client.

The Cisco eNcore client Collects System intrusion, discovery, and connection data from the Firepower Management Center or managed device (also referred to as the eStreamer server) to external client applications, in this case via Syslog to FortiSIEM.

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Using Cisco eStreamer Client

What is Discovered and Monitored

Protocol	Information Discovered	Logs Collected	Used For
eStreamer API		Intrusion Events, Malware Events. File Events. Discovery Events, User Activity Events, Impact Flag Events	Security Monitoring

Event Types

FortiSIEM obtains events from Cisco FireSIGHT via eStreamer protocol. Event types follow.

- **Intrusion events**: PH_DEV_MON_FIREAMP_INTRUSION

```
[PH_DEV_MON_FIREAMP_INTRUSION]:[eventSeverity]=PHL_CRITICAL,
[fileName]=phFireAMPAgent.cpp,[lineNumber]=381,[reptDevIpAddr]=10.1.23.177,
[envSensorId]=6,[snortEventId]=393258,[deviceTime]=1430501705,[eventType]=Snort-1,
[compEventType]=PH_DEV_MON_FIREAMP_INTRUSION,[ipsGeneratorId]=137,[ipsSignatureId]=2,
[ipsClassificationId]=32,[srcIpAddr]=10.131.10.1,[destIpAddr]=10.131.10.120,
[srcIpPort]=34730,[destIpPort]=443,[ipProto]=6,[iocNum]=0,[fireAmpImpactFlag]=7,
[fireAmpImpact]=2,[eventAction]=1,[mplsLabel]=0,[hostVLAN]=0,[userId]=3013,[webAppId]=0,
[clientAppId]=1296,[appProtoId]=1122,[fwRule]=133,[ipsPolicyId]=63098,
[srcIntfName]=b16c69fc-cd95-11e4-a8b0-b61685955f02,[destIntfName]=b1a1f900-cd95-11e4-
a8b0-b61685955f02,[srcFwZone]=9e34052a-9b4f-11e4-9b83-efa88d47586f,
[destFwZone]=a7bd89cc-9b4f-11e4-8260-63a98d47586f,[connEventTime]=1430501705,
[connCounter]=371,[srcGeoCountryCode]=0,[destGeoCountryCode]=0,[phLogDetail]=
```

- **Malware events**: PH_DEV_MON_FIREAMP_MALWARE

```
[PH_DEV_MON_FIREAMP_MALWARE]:[eventSeverity]=PHL_INFO,[fileName]=phFireAMPAgent.cpp,
[lineNumber]=487,[reptDevIpAddr]=10.1.23.177,[envSensorId]=6,[deviceTime]=1430502934,
[srcIpAddr]=10.110.10.73,[destIpAddr]=10.0.112.132,[srcIpPort]=21496,[destIpPort]=80,
[ipProto]=6,[fileName]=CplLnk.exe ,[filePath]=,[fileSize64]=716325,[fileType]=1,
[fileTimestamp]=0,[hashAlgo]=SHA,
[hashCode]=f1bfab10090541a2c3e58b4b93c504be8b65cdc823209c7f4def24acc38d7fd1 ,
[fileDirection]=1,[fireAmpFileAction]=3,[parentFileName]=,[parentFileHashCode]=,
[infoURL]=http://wrl/wrl/CplLnk.exe ,[threatScore]=0,[fireAmpDisposition]=3,
[fireAmpRetrospectiveDisposition]=3,[iocNum]=1,[accessCtlPolicyId]=125870424,
[srcGeoCountryCode]=0,[destGeoCountryCode]=0,[webAppId]=0,[clientAppId]=638,
[applicationId]=676,[connEventTime]=1430502933,[connCounter]=409,[cloudSecIntelId]=0,
[phLogDetail]=
```

- **File events**: PH_DEV_MON_FIREAMP_FILE

  ```
  [PH_DEV_MON_FIREAMP_FILE]:[eventSeverity]=PHL_INFO,[fileName]=phFireAMPAgent.cpp,
  [lineNumber]=541,[reptDevIpAddr]=10.1.23.177,[envSensorId]=6,[deviceTime]=1430497343,
  [srcIpAddr]=10.131.15.139,[destIpAddr]=10.0.112.137,[srcIpPort]=1587,[destIpPort]=80,
  [ipProto]=6,[fileName]=Locksky.exe ,[hashAlgo]=SHA,
  [hashCode]=aa999f5d948aa1a731f6717484e1db32abf92fdb5f1e7ed73ad6f5a21b0737c1,
  [fileSize64]=60905,[fileDirection]=1,[fireAmpDisposition]=3,[fireAmpSperoDisposition]=4,
  [fireAmpFileStorageStatus]=11,[fireAmpFileAnalysisStatus]=0,[threatScore]=0,
  [fireAmpFileAction]=3,[fileType]=17,[applicationId]=676,[destUserId]=2991,
  [infoURL]=http://wrl/wrl/Locksky.exe ,[signatureName]=,[accessCtlPolicyId]=125869976,
  [srcGeoCountryCode]=0,[destGeoCountryCode]=0,[webAppId]=0,[clientAppId]=638,
  [connCounter]=103,[connEventTime]=1430497343,[phLogDetail]=
  ```

- **Discovery events**:
  - PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL

    ```
    PH_DEV_MON_FIREAMP_DISCOVERY_NETWORK_PROTOCOL]:[eventSeverity]=PHL_INFO,
    [fileName]=phFireAMPAgent.cpp,[lineNumber]=815,[reptDevIpAddr]=10.1.23.177,
    [destIpPort]=2054,[ipProto]=54,[phLogDetail]=
    ```

  - PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT

    ```
    [PH_DEV_MON_FIREAMP_DISCOVERY_OS_FINGERPRINT]:[eventSeverity]=PHL_INFO,
    [fileName]=phFireAMPAgent.cpp,[lineNumber]=737,[reptDevIpAddr]=10.1.23.177,
    [fingerprintId]=01f772b2-fceb-4777-8a50-1e1f27426ad0,[osType]=Windows 7,
    [hostVendor]=Microsoft,[osVersion]=NULL,[phLogDetail]=
    ```

  - PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP

    ```
    [PH_DEV_MON_FIREAMP_DISCOVERY_CLIENT_APP]:[eventSeverity]=PHL_INFO,
    [fileName]=phFireAMPAgent.cpp,[lineNumber]=775,[reptDevIpAddr]=10.1.23.177,
    [clientAppId]=638,[appName]=Firefox,[phLogDetail]=
    ```

  - PH_DEV_MON_FIREAMP_DISCOVERY_SERVER

    ```
    [PH_DEV_MON_FIREAMP_DISCOVERY_SERVER]:[eventSeverity]=PHL_INFO,
    [fileName]=phFireAMPAgent.cpp,[lineNumber]=853,[reptDevIpAddr]=10.1.23.177,
    [applicationId]=676,[appTransportProto]=HTTP,[phLogDetail]=
    ```

- **User activity events**: PH_DEV_MON_FIREAMP_USER_LOGIN

  ```
  [PH_DEV_MON_FIREAMP_USER_LOGIN]:[eventSeverity]=PHL_INFO,[fileName]=phFireAMPAgent.cpp,
  [lineNumber]=672,[reptDevIpAddr]=10.1.23.177,[deviceTime]=1430490441,[user]=ABerglund ,
  [userId]=0,[ipProto]=710,[emailId]=,[loginType]=0,[destIpAddr]=198.18.133.1 ,
  [phLogDetail]=
  ```

- **Impact Flag events**: PH_DEV_MON_FIREAMP_IMPACT_FLAG

```
[PH_DEV_MON_FIREAMP_IMPACT_FLAG]:[eventSeverity]=PHL_CRITICAL,
[fileName]=phFireAMPAgent.cpp,[lineNumber]=591,[reptDevIpAddr]=10.1.23.177,
[envSensorId]=6,[snortEventId]=34,[deviceTime]=1430491431,[eventType]=Snort-648,
[compEventType]=PH_DEV_MON_FIREAMP_IMPACT_FLAG,[ipsGeneratorId]=1,[ipsSignatureId]=14,
[ipsClassificationId]=29,[srcIpAddr]=10.131.12.240,[destIpAddr]=10.131.11.46,
[srcIpPort]=80,[destIpPort]=8964,[ipProto]=6,[fireAmpImpactFlag]=7,[phLogDetail]=
```

Rules

There are no predefined rules for this device.

Reports

The following reports are provided:

- Top Cisco FireAMP Malware Events
- Top Cisco FireAMP File Analysis Events
- Top Cisco FireAMP Vulnerable Intrusion Events
- Top Cisco FireAMP Discovered Login Events
- Top Cisco FireAMP Discovered Network Protocol
- Top Cisco FireAMP Discovered Client App
- Top Cisco FireAMP Discovered OS

Configuration

- Cisco FireSIGHT Configuration
- FortiSIEM Configuration

Cisco FireSIGHT Configuration

1. Login to Cisco FIRESIGHT console.
2. Go to **System** > **Local** > **Registration** > **eStreamer**
3. Click **Create Client**
   a. Enter **IP address** and **Password** for FortiSIEM. The password can only contain alpha (a-z, A-Z) and numeric (0-9) characters. Special characters are not allowed.
   b. Click **Save**.
4. Select the types of events that should be forwarded to FortiSIEM.
5. Click **Download Certificate** and save the certificate to a local file.

FortiSIEM Configuration

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

- Define Cisco FireSIGHT console and FirePower Threat Defense Credential in FortiSIEM
- Create IP Range to Credential Association and Test Connectivity

Define Cisco FireSIGHT console and FirePower Threat Defense Credential in FortiSIEM

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   - **a.** Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   - **b.** Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Cisco FireAMP
Access Protocol	eStreamer SDK
Password	Enter the **Password** as in Step 3a from Cisco FireSIGHT Configuration.
Certificate File	Click **Upload** and enter/select the certificate downloaded in Step 5 from Cisco FireSIGHT Configuration.
Organization	The organization the device belongs to.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   - **a.** Enter the IP address of the FireSIGHT console in the **IP/Host Name** field.
   - **b.** Select the name of the credential created in Define Cisco FireSIGHT console and FirePower Threat Defense Credential in FortiSIEM from the **Credentials** drop-down list.
   - **c.** Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity**. FortiSIEM will start collecting events from the FIRESIGHT console.

Using Cisco eStreamer Client

Cisco has published a free eStreamer client to pull events from FireAMP server. This client is more up-to-date than FortiSIEM’s own eStreamer client.

If you decide to use Cisco’s eStreamer client instead of FortiSIEM’s eStreamer client, follow these steps.

- Step 1: Install a New Version of Python with a New User 'estreamer'
- Step 2: Download and Configure eStreamer Client
- Step 3: Start eStreamer Client

Step 1: Install a New Version of Python with a New User 'estreamer'

This is required because the python version used by FortiSIEM is compiled with PyUnicodeUCS2, while eStreamer client requires the standard version of python built with PyUnicodeUCS4.

1. Log in to FortiSIEM Collector or the node where eStreamer client is going to be installed.
2. Install openssl-devel and openssl-devel.i686 by running the following command.
   `yum install openssl-devel openssl-devel.i686`
3. Create eStreamer user using the following command.
   a. `useradd estreamer`
4. Download the python library using the following commands.
   a. `su estreamer`
   b. `mkdir ~/python`
   c. `cd ~/python`
   d. `wget https://www.python.org/ftp/python/2.7.18/Python-2.7.18.tgz`
5. Install python library by using the following commands.
   a. `tar zxfv Python-2.7.18.tgz`
   b. `find ~/python -type d | xargs chmod 0755`
   c. `cd Python-2.7.18`
   d. `./configure --prefix=$HOME/python --enable-unicode=ucs4`
   e. `make && make install`
   f. Add the following two lines to `~/.bashrcp`.
   ```
   export PATH=$HOME/python/Python-2.7.18/:$PATH
   export PYTHONPATH=$HOME/python/Python-2.7.18
   ```
   g. `source ~/.bashrc`

Step 2: Download and Configure eStreamer Client

1. SSH to FortiSIEM Collector or the node where eStreamer client is going to be installed as estreamer user.
2. Git clone: git://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight.git
3. Change directory using the following command.
   `cd fp-05-firepower-cef-connector-arcsight`
4. Login to eStreamer server and take the following steps.
   a. Go to **System** > **Integration** > **eStreamer**.
   b. Create a **New client** and enter the **IP address** of the Supervisor/Collector as the host.
   c. Download the pkcs12 file and save it to directory.
   `fp-05-firepower-cef-connector-arcsight`
5. Go back to `fp-05-firepower-cef-connector-arcsight` directory.
6. Run `sh encore.sh`, and type `2` for selection of output in CEF as prompted. An estreamer.conf file is generated.
7. Edit estreamer.conf with the below settings (in JSON format).
   - `handler.outputters.stream.uri : "udp://VA_IP:514"`
   - `servers.host : eStreamer_Server_IP`
   - `servers.pkcs12Filepath : /path/to/pkcs12`
8. Run the following two commands.
   - `openssl pkcs12 -in "client.pkcs12" -nocerts -nodes -out "/path/to/fp-05-firepower-cef-connector-arcsight/{`*`eStreamer_Server_IP`*`}-{`*`port`*`}_pkcs.key"`

- `openssl pkcs12 -in "client.pkcs12" -clcerts -nokeys -out "/path/to/fp-05-firepower-cef-connector-arcsight/{eStreamer_Server_IP}-{port}_pkcs.cert"`

Notes:

1. 8302 is the default port.
2. The public IP of the device must be used to create `client.pkcs12` according to Cisco FireSIGHT Configuration documentation. The command `curl ifconfig.co` can be used to get the public IP of the device.

Step 3: Start eStreamer Client

SSH to FortiSIEM Collector or the node where eStreamer client is installed, as eStreamer user. Start eStreamer client by entering:

```
sh encore.sh start
```

Now eStreamer client is ready for use. FortiSIEM 5.2.5 contains an updated parser for the events generated by Cisco eStreamer client. Trigger a few events in eStreamer server and query from FortiSIEM to verify if everything is working.

Cisco Intrusion Prevention System

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			Performance and Availability Monitoring
SDEE		Alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco ips" in the **Search...** field to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "cisco ips" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "cisco ips" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

1. Log in to the device manager for your Cisco IPS.
2. Go to **Configuration > Allowed Hosts/Networks**.
3. Click **Add**.
4. Enter the IP address of your FortiSIEM virtual appliance to add it to the access control list, and then click **OK.**
5. Go to **Configuration > Sensor Management > SNMP > General Configuration**.

6. For **Read-Only Community String**, enter `public`.
7. For **Sensor Contact** and **Sensor Location**, enter **Unknown**.
8. For **Sensor Agent Port**, enter **161**.
9. For **Sensor Agent Protocol**, select **udp**.

If you must create an SDEE account for FortiSIEM to use, go to **Configuration > Users** and **Add** a new administrator.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco IPS
Access Protocol	Cisco SDEE
Pull Interval	5 minutes
Port	443
Password config	See Password Configuration

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Sample XML-Formatted Alert

```
<\!-\- CISCO IPS \--><evAlert eventId="1203541079317487802" severity="low"> <originator>
     <hostId>MainFW-IPS</hostId> <appName>sensorApp</appName>
     <appInstanceId>376</appInstanceId> </originator> <time offset="0"
     timeZone="UTC">1204938398491122000</time> <signature sigName="ICMP Network Sweep
     w/Echo" sigId="2100" subSigId="0" version="S2"></signature>
     <interfaceGroup>vs1</interfaceGroup><vlan>0</vlan> <participants> <attack> <attacker>
     <addr locality="OUT">2.2.2.1</addr> </attacker> <victim> <addr
     locality="OUT">171.64.10.225</addr> <os idSource="unknown" type="unknown"
     relevance="relevant"></os> </victim> <victim> <addr
     locality="OUT">171.66.255.87</addr> <os idSource="unknown" type="unknown"
     relevance="relevant"></os> </victim> <victim> <addr
     locality="OUT">171.66.255.86</addr> <os idSource="unknown" type="unknown"
     relevance="relevant"></os> </victim> <victim> <addr
```

```
locality="OUT">171.66.255.84</addr> <os idSource="unknown" type="unknown"
relevance="relevant"></os> </victim> <victim> <addr
locality="OUT">171.66.255.85</addr> <os idSource="unknown" type="unknown"
relevance="relevant"></os> </victim> <victim> <addr
locality="OUT">171.66.255.82</addr> <os idSource="unknown" type="unknown"
relevance="relevant"></os> </victim> </attack> </participants>
<alertDetails>InterfaceAttributes: context="single_vf" physical="Unknown"
backplane="GigabitEthernet0/1" </alertDetails></evAlert>
```

Cisco Stealthwatch

- Integration Points
- Event Types
- Configuring FortiSIEM

Integration Points

Protocol	Information Discovered	Used For
syslog	Network Anomaly Detection Alerts	Security and Compliance

Event Types

Currently over 150 events are parsed. See event types in **RESOURCES > Event Types**, and search for "Cisco-StealthWatch-" in the main content panel **Search...** field. The user can extend the parser to add other events.

Configuring FortiSIEM

FortiSIEM automatically recognizes Cisco Stealthwatch syslog as long as it follows the format as shown in the sample syslog:

```
<129>Jun 18 14:56:00 ED2ALENTSVRSMC-1 StealthWatch[2699]: Lancope|StealthWatch|PRIORITY
A|time=2018-06-18T14:55:30Z|target_hostname=|alarm_severity_id=5|alarm_type_
id=60|alarm_type_description=Host may be infected with an SMB
```

Claroty Continuous Threat Detection (CTD) Platform

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Claroty Alert, Baseline and Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "ClarotyCTD" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 20 event types defined.

Rules

There are no specific rules available for Claroty.

Reports

There are no specific reports available for Claroty. You can view all Claroty events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "ClarotyCTD".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<12>Sep 12 15:31:33 localhost.localdomain
CEF:0|Claroty|CTD|2.7.0|Baseline|None|Unapproved|cs1Label=Site cs1=Site cs2Label=Network
cs2=Default cs3Label=Transmission cs3=TCP / 44818 cs4Label=SiteId cs4=1 cs5Label=SrcZone
cs5=Engineering Station: Rockwell cs6Label=DstZone cs6=PLC: Rockwell cs7Label=Category
cs7=Protocol cs8Label=CategoryAccess cs8=Read cs9Label=Frequency cs9=NotTimed
cs10Label=FirstSeen cs10=Sep 12 2018 15:31:29 src=10.1.30.40 smac=00:50:56:b9:e2:ad
shost=N/A dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d dhost=N/A externalId=2365 cat=Create rt=Sep
12 2018 15:31:29 msg=CIP : Service Get Attribute All called on ExtendedDevice
```

```
<12>Sep 12 15:18:03 localhost.localdomain CEF:0|Claroty|CTD|2.7.0|Alert|Configuration
Download|Critical|cs1Label=Site cs1=Site cs2Label=Network cs2=Default cs3Label=ResolvedAs
cs3=Unresolved cs4Label=SiteId cs4=1 cs5Label=SrcZone cs5=Engineering Station: Rockwell
cs6Label=DstZone cs6=PLC: Rockwell cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8=https://10.210.16.2:5000/alert/74-1 src=10.1.30.40 smac=00:50:56:b9:e2:ad shost=N/A
dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d dhost=N/A externalId=74 cat=Create rt=Sep 12 2018
15:18:01 msg=A configuration has been downloaded to controller Chemical_plant by 10.1.30.40
```

Corero Smartwall Threat Defense System

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Security Alerts and Events	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Corero-smart" to see the event types associated with this device. In FortiSIEM 6.2.0, there are approximately 3,452 event types defined.

Rules

There are no specific rules available for Corero.

Reports

There are no specific reports available for Corero. You can view all Corero events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Corero-smart".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Please refer to the Corero documentation for information on configuring the device at the following link.

https://www.juniper.net/documentation/en_US/corero-smartwall9.5.0/information-products/topic-collections/Corero_SmartWall_CMS_UG/Content/cms_connect_swa.htm

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Corero SmartWall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sample Syslog

```
<165>2020-09-22T18:07:28.905+02:00 10.11.12.13
cat=network,type=sflow,v=1,cl=default,device=Defense_10_12_12_
102,profile=default,sc=175,sfn=16,dir=inbound,time=1600790847976000,mp=xe-
1/1,issr=1999,isr=1,px=32,lb=0,ipv=4,dip=1.2.3.4,dprt=61205,iplen=1143,prot=6,tos=0,sip=1.2.
3.5,sprt=443,ttl=126,bp=0,ep=0,icn=5,scl=0,fp=0,flags=24,flags-
decode=PSH:ACK,plen=1161,ptag=37,pdu=0896ad670b22204e71624fc68100002508004500047762f400007e0
6f701d83ad724b9b9757201bbef15d173297cf6bf83c7501810dec0ad00004b10a65f2b244bb73879b0f43464282
73ce3582fe59501013ea113a6bbdc535832cbf1ea85d95ecd7ab906eae299b27f16ee3d74b7fe3d981e33971dad0
e03d68f90c03fbfabbd4fb63d081701603f5893e42ef3311b0d4936e9abd39621f62608de62b4466947feeaf3ca9
aca54ba8fb8121dd3b5dfa5a3adf0ca8c92bb3cf4398b15edb508901db78409a09e3c
```

Cylance Protect Endpoint Protection

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Example Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		End point malware alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cylance" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via **CEF formatted syslog** sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>

Setting	Value
Device Type	Cylance Protect
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
CylancePROTECT: Event Type: AppControl, Event Name: pechange, Device Name: WIN-7entSh64, IP
Address: (192.168.119.128), Action: PEFileChange, Action Type: Deny, File Path:
C:\Users\admin\AppData\Local\Temp\MyInstaller.exe, SHA256:
04D4DC02D96673ECA9050FE7201044FDB380E3CFE0D727E93DB35A709B45EDAA
```

Cyphort Cortex Endpoint Protection

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Example Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		End point malware alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "cyphort" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via **CEF formatted syslog** sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>

Setting	Value
Device Type	Cylance Cortex
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<134>Feb 23 21:58:05 tap54.eng.cyphort.com cyphort:
CEF:0|Cyphort|Cortex|3.2.1.16|http|TROJAN_GIPPERS.DC|8|externalId=374 eventId=13348
lastActivityTime=2015-02-24 05:58:05.151123+00 src=172.16.0.1 dst=10.1.1.26
fileHash=acf69d292d2928c5ddfe5e6af562cd482e6812dc
fileName=79ea1163c0844a2d2b6884a31fc32cc4.bin fileType=PE32 executable (GUI) Intel 80386,
for MS Windows startTime=2015-02-24 05:58:05.151123+00
```

Damballa Failsafe

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, and click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	A name for the device.
Device Type	Damballa Failsafe
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Damballa Failsafe.
5. To see the jobs associated with Damballa, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Damballa" in the search box.

Darktrace CyberIntelligence Platform

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOGs collected	Used for
Syslog (CEF formatted)		Over 40 security logs	Security and Compliance monitoring

Event Types

Go to **ADMIN > Device Support > Event Types** and search for "Darktrace-DCIP" to see the event types associated with this device.

Rules

None

Reports

None

Configuration

Configure Darktrace to send CEF formatted logs to FortiSIEM. FortiSIEM will automatically parse the logs. No configuration is required in FortiSIEM.

Sample Events

```
CEF:0|Darktrace|DCIP|3.0.8|537|Antigena/Network/Compliance/Antigena RDP Block|Low| eventId=2
externalId=1462565 art=1536856095244 deviceSeverity=1 rt=1536856054000
shost=personalpcd698.abccompany.local src=10.10.1.85 sourceZoneURI=/All Zones/ArcSight
System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 smac=1:1:1:1:1:1
dst=1.1.1.1 destinationZoneURI=/All Zones/ArcSight System/Public Address Space
Zones/APNIC/1.0.0.0-1.1.1.255 (APNIC) dpt=9999 ahost=personalpc123.abccompany.local
agt=10.10.28.38 agentZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918:
```

```
10.0.0.0-10.255.255.255 av=2.2.2.2.0 atz=CountryA aid=3mAvC02UBABCAa72iNm4jZA\=\= at=syslog
dvc=10.10.10.10 deviceZoneURI=/All Zones/ArcSight System/Private Address Space
Zones/RFC1918: 10.0.0.0-10.255.255.255 dtz=CountryA _cefVer=0.1
ad.darktraceUrl=https://10.10.10.10/#modelbreach/1462565
```

Dragos Platform

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Dragos Alert logs regarding Modeling, Indicator, Configuration, Threat Behavior	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "dragos" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 5 event types defined.

Rules

There are no specific rules available for Dragos.

Reports

There are no specific reports available for Dragos.

There are no specific reports available for Dragos. You can view all Dragos events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Dragos".

6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<13>1 2020-07-02T14:58:31.538019Z dragos dragos_syslog - - system="Dragos Platform"
createdAt="2020-07-02T14:58:31Z" summary="Test Message from Dragos App" severity="
{severity}" content="This test message was created by the Dragos Syslog App" asset_ip=#"
{asset_ip}" asset_hostname="Test" dst_asset_ip="10.0.0.9" dst_asset_hostname="Test" dst_
asset_mac="83:77:DB:E3:A3:38" dst_asset_domain="ip-10-10-255-1.ec2.test" src_asset_
ip="10.0.0.9" src_asset_hostname="Test" src_asset_mac="89:3A:EE:01:0F:D3" src_asset_
domain="ip-10-10-test.ec2.test" id="1234567" asset_domain="ip-10-10-255-1.ec2.test" asset_
id="111111" asset_mac="06:92:1C:1B:F2:72" detection_quad="Modeling" detectorId="test-
detector-1111" dst_asset_id="333333" matchedRuleId="16" occurredAt="2020-07-02T14:58:31Z"
originalSeverity="0" reviewed="False" src_asset_id="222222" type="Test"
```

```
<8>May 06 21:06:19 dragos dragos_syslog: CEF:0|Dragos|Platform|1.6|notification|Test Message
from Dragos App|5|content=This test message was created by the Dragos Syslog App asset_
ip=10.0.0.9 asset_hostname=Test dst_asset_ip=10.0.0.9 dst_asset_hostname=Test dst_asset_
mac=9C:B6:TE:ST:4B:95 dst_asset_domain=ip-10-10-255-1.ec2.test src_asset_ip=10.0.0.9 src_
asset_hostname=Test src_asset_mac=TE:ST:D0:F2:4B:95 src_asset_domain=ip-10-10-test.ec2.test
id=1234567 asset_domain=ip-10-10-255-1.ec2.test asset_id=111111 asset_mac=9C:B6:D0:F2:TE:ST
createdAt=2020-05-06T21:06:24Z detection_quad=Indicator detectorId=test-detector-4444 dst_
asset_id=333333 matchedRuleId=16 occurredAt=2020-05-06T21:06:24Z originalSeverity=5
reviewed=False src_asset_id=222222 type=Test
```

FireEye Malware Protection System (MPS)

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "fireeye" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	FireEye MPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<164>fenotify-45640.alert: CEF:0|FireEye|MPS|6.0.0.62528|MC|malware-callback|9|rt=Apr 16
2012 15:54:41 src=192.168.26.142 spt=0 smac=00:14:f1:90:c8:01 dst=2.2.2.2 dpt=80
dmac=00:10:db:ff:50:00 cn1Label=vlan cn1=202 cn2Label=sid cn2=33335390 cs1Label=sname
cs1=Trojan.Gen.MFC cs4Label=link cs4=https://10.10.10.10/event_stream/events_for_bot?ev_
id\=45640 cs5Label=ccName cs5=3.3.3.3 cn3Label=ccPort cn3=80 proto=tcp cs6Label=ccChannel
cs6= shost=abc.org <http://abc.org>  dvchost=ALAXFEYE01 dvc=10.10.10.10 externalId=45640
```

FortiDDoS

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog	Host Name, Access IP, Vendor/Model	Over 150 event types to include Protocol Anomaly, Traffic Volume Anomaly, DoS Attacks,	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiDDoS" to see the event types associated with this device.

Rules

There are many IPS correlation rules for this device under **RESOURCES > Rules > Security > Exploits**.

Reports

There are many reports for this device under **RESOURCES > Reports > Function > Security**.

Configuration

Syslog

FortiSIEM processes FortiDDoS events via syslog. Configure FortiDDoS to send syslog to FortiSIEM as directed in the device's product documentation by taking the following steps:

FortiDDOS documentation available here: https://help.fortinet.com/fddos/4-7-0/index.htm#fortiddos/Configuring_remote_log_server_settings_for_event_l.htm

1. Navigate to **Log & Report > Event Log Remote**.
2. Click **Add**.
3. Complete the configuration.
4. Click **Save**.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiDDos
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
Jan 10 16:01:50 172.30.84.114 devid=FI400B3913000032 date=2015-01-23 time=17:42:00
type=attack SPP=1 evecode=1 evesubcode=8 dir=0 protocol=1 sIP=0.0.0.0 dIP=0.0.0.0
dropCount=312
devid=FI800B3913000055 date=2017-01-27 time=18:24:00 tz=PST type=attack spp=0 evecode=2
evesubcode=61 description="Excessive Concurrent Connections Per Source flood" dir=1
sip=24.0.0.2 dip=24.255.0.253 subnet_name=default dropcount=40249 facility=Local0
level=Notice
```

Fortinet FortiDeceptor

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Authentication logs, Decoy activity	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiDeceptor" to see the event types associated with this device.

Rules

No specific rules are written for FortiDeceptor.

Reports

No specific reports are written for FortiDeceptor.

Configuration

Configure FortiDeceptor system to send logs to FortiSIEM in the supported format (see Sample Events).

Refer to the latest FortiDeceptor Administration Guide for the latest configuration steps. Instructions here have been taken from the 3.3.1 FortiDeceptor Administration Guide.

To configure syslog in FortiDeceptor, take the following steps:

1. From FortiDeceptor, navigate to **Log > Log Servers**.
2. Click **Create New** and enter the following information into the configuration.

Field	**Input**
Name	FortiSIEM

Field	Input
Server Type	syslog
Server Address	Input the IP address or FQDN of your FortiSIEM collector.
Port	Leave as default (UDP 514)
Status	Enabled
Log Level	Information

3. If applicable, click **OK**.

Settings for Access Credentials

None required.

Sample Events

```
<27>2019-07-29T10:12:44 devhost=FDC-VM0000000262 devid=FDC-VM0000000262 logver=25
     tzone=14400 tz=GST date=2019-07-29
time=10:12:44 logid=0106000001 type=event subtype=system level=error user=system ui=GUI
     action=update status=failure
msg="The authentication to FDN server failed"

<14>2019-07-29T10:40:34 devhost=FDC-VM0000000262 devid=FDC-VM0000000262 logver=25
     tzone=14400 tz=GST date=2019-07-29
time=10:40:34 logid=0106000001 type=event subtype=system level=information user=admin ui=GUI
     action=Login
status=success msg="Administrator admin logged into website successfully from 10.0.0.254"
```

Fortinet FortiNAC

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Administrative and User Admission Control events	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiNAC" to see the event types associated with this device.

Rules

No specific rules are written for FortiNAC but generic rules for network admission control apply

Reports

No specific reports are written for FortiNAC but generic reports for network admission control apply Configuration

Configuration

Configure FortiNAC system to send logs to FortiSIEM in the supported format (see Sample Events).

To configure FortiNAC to send syslog to FortiSIEM, take the following steps:

Note: Refer to the latest FortiNAC Administration Guide for the latest instructions. Steps provided here to configure syslog for FortiSIEM are from the 9.1.0 FortiNAC Administration Guide.

1. Click **System > Settings**.
2. In the left navigation tree, select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.

4. Enter the configuration parameters from the following table to configure:

Field	Definition
Type	Select **Syslog Command Event Format (CEF)** for FortiSIEM configuration.
IP address	Provide the IP address of the FortiSIEM Collector that will receive Event and Alarm messages.
Port	The default port for Syslog CEF servers is **514**. Leave as is.
Facility	Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is **4 security/authorization messages**. Leave as is.

5. Click **OK**.

Settings for Access Credentials

None required.

Sample Events

```
<37>Jan 08 19:03:45 : CEF:0|Bradford Networks|FortiNAC-VM-Control and Application
     Server|8.3.0.79|426|
Adapter Destroyed|1|rt=Jan 08 19:03:45 269 UTC cat=EndStation msg=Adapter 18:5E:0F:AA:56:31
     Destroyed.

<37>Dec 06 10:34:42 : CEF:0|Bradford Networks|FortiNAC-VM-Control and Application Server|
8.3.1.30|447702|Admin User Login Success|1|rt=Dec 06 10:34:42 736 CET
cat= suid=guiadmin msg=Admin user guiadmin logged in.

<37>Apr 16 11:06:19 : CEF:0|Bradford Networks|FortiNAC-VM-Control and Application
     Server|8.3.6.104|605250|
Security Risk Host|1|rt=Apr 16 11:06:19 447 CEST cat=EndStation src=192.168.242.20
     smac=00:26:9E:D9:87:12
shost=X100e-1 cs1Label=Physical<space>network<space>location cs1=BA-HPswitch
     GigabitEthernet1/0/10
{ GigabitEthernet1/0/10 Interface } msg=Host failed Windows-PA-Notepad Tests: Failed ::
     Custom :: Notepad
MAC Address: 00:26:9E:D9:87:12 Last Known Adapter IP: 192.168.242.20 Host Location: BA-
     HPswitch
GigabitEthernet1/0/10 { GigabitEthernet1/0/10 Interface }
```

Fortinet FortiSandbox

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP	Host Name, OS, version, Hardware	CPU, Memory, Disk, Interface utilization	Performance Monitoring
HTTP(S)	Host Name, OS, version, Hardware		Log Management, Security Compliance, SIEM
Syslog	Threat feed - Malware URL, Malware Hash	Malware found/cleaned, Botnet, Malware URL, System Events	Log Management, Security Compliance, SIEM

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortisandbox-" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortisandbox" in the main content panel **Search...** field to see the rules associated with this device.

Also, basic availability rules in **RESOURCES > Rules > Availability > Network** and performance rules in **RESOURCES > Rules> Performance > Network** also trigger.

Reports

In **RESOURCES > Reports**, search for "fortisandbox" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

For FortiSandbox log server documentation, see https://docs.fortinet.com/document/fortisandbox/4.0.0/administration-guide/323679/log-servers.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog format should be the same as that shown in the example.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiSandbox
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
Oct 12 14:35:12 172.16.69.142 devname=turnoff-2016-10-11-18-46-05-172.16.69.142 device_
id=FSA3KE3A13000011 logid=0106000001 type=event subtype=system pri=debug user=system
ui=system action= status=success reason=none letype=9 msg="Malware package: urlrel version
2.88897 successfully released, total 1000"
<14>2016-08-19T06:48:51 devhost=turnoff-2016-08-15-19-24-55-172.16.69.55
devid=FSA35D0000000006 tzone=-25200 tz=PDT date=2016-08-19 time=06:48:51 logid=0106000001
type=event subtype=system level=information user=admin ui=GUI action=update status=success
reason=none letype=9 msg="Remote log server was successfully added"
```

Fortinet FortiTester

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Syslog (CEF formatted)	Host name and Device Type from LOG	Over 14 log types	Security and Compliance

Event Types

Go to **ADMIN > Device Support > Event Types**, and search for "FortiTester" to see the event types associated with this device.

Rules

None

Reports

None

Configuration

Configure FortiTester to send CEF formatted syslog to FortiSIEM. No configuration is required on FortiSIEM.

Sample Events

```
CEF:0|Fortinet|FortiTester|3.8|Event|information|category=System
deviceExternalId=FTS2KET618000005 msg=The system is started deviceCustomDate1=2019-11-05-
15:12:30 cs1= cs1Label=Description
```

IBM Internet Security Series Proventia

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected
SNMP Traps		

Event Types

In **ADMIN > Device Support > Event Types**, search for "proventia" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP Trap
- Define FortiSIEM as a Response Object for SNMP Traps
- Define a Response Rule to Forward SNMP Traps to FortiSIEM
- Refining Rules for Specific IP Addresses

SNMP Trap

FortiSIEM receives SNMP traps from IBM/ISS Proventia IPS appliances that are sent by IBM/ISS SiteProtector Management Console. You must first configure IBM/ISS Proventia to send alerts to IBM/ISS SiteProtector, then configure IBM/ISS SiteProtector to send those alerts as SNMP traps to FortiSIEM.

Configure IBM/ISS Proventia Appliances to Send SNMP Notifications to IBM/ISS SiteProtector Management Console

1. Log in to the IBM Proventia IPS web interface.
2. Click **Manage System Settings > SiteProtector Management.**
3. Click and select **Register withSiteProtector**.
4. Click and select **Local Settings Override SiteProtector Group Settings**.
5. Specify the **Group**, **Heartbeat Interval**, and **Logging Level**.
6. Configure these settings:

Setting	Description
Authentication Level	Use the default **first-time trust.**
Agent Manager Name	Enter the Agent Manager name exactly as it appears in SiteProtector. This setting is case-sensitive.
Agent Manager Address	Enter the Agent Manager's IP address.
Agent Manager Port	Use the default value **3995**.
User Name	If the appliance has to log into an account access the Agent Manager, enter the user name for that account here.
User Password	Click Set Password, enter and confirm the password, and then click **OK.**
Use Proxy Settings	If the appliance has to go through a proxy to access the Agent Manager, select the **Use Proxy Settings** option, and then enter the **Proxy Server Address** and **Proxy Server Port**.

Define FortiSIEM as a Response Object for SNMP Traps

1. Log in to IBM SiteProtector console.
2. Go to **Grouping > Site Management > Central Responses > Edit settings**.
3. Select **Response Objects > SNMP**.
4. Click **Add**.
5. Enter a **Name** for your FortiSIEM virtual appliance.
6. For **Manager**, enter the IP address of your virtual appliance.
7. For **Community**, enter `public`.
8. Click **OK.**

Define a Response Rule to Forward SNMP Traps to FortiSIEM

1. Go to **Response Rules.**
2. Click **Add.**
3. Select **Enabled.**

4. Enter a **Name** and **Comment** for the response rule.
5. In the **Responses** tab, select **SNMP**.
6. Select **Enabled** for the response object that represents your FortiSIEM virtual appliance.
7. Click **OK**.

Refining Rules for Specific IP Addresses

By default, a rule matches on any source or destination IP addresses.

1. To refine the rule to match on a specific source IP address, select the rule, click **Edit**, and then select the **Source** tab.
2. Select **Use specific source addresses** to restrict the rule based on IP address of the source.
   If you set this option, set the **Mode** to specify that the rule should either be **From** or **Not From** the IP address.
3. Click **Add** to define one or more IP addresses.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	IBM ISS Proventia
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sample SNMP Trap

```
2013-02-07 16:52:18 100.0.0.218(via UDP: [192.168.64.218]:55545) TRAP, SNMP v1,
community public SNMPv2-SMI::enterprises.2499 Enterprise Specific Trap (4) Uptime:
0:00:00.15 SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.1 = STRING: "SiteProtector_
Central_Response (Response1)" SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.2 = STRING:
"16:52:18 2013-02-07" SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.3 = STRING: "6"
SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.4 = STRING: "100.0.0.216" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.5 = STRING: "100.0.0.218" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.6 = "" SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.7
= "" SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.8 = STRING: "48879" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.9 = STRING: "80" SNMPv2-
SMI::enterprises.2499.1.1.2.1.1.1.1.10 = STRING: "DISPLAY=WithoutRaw:0,BLOCK=Default:0"
SNMPv2-SMI::enterprises.2499.1.1.2.1.1.1.1.11 = STRING: " SensorName: IBM-IPS
ObjectName: 80 DestinationAddress: 100.0.0.218 AlertName: HTTP_OracleAdmin_Web_
Interface AlertTarget: 100.0.0.218 AlertCount: 1 VulnStatus: Simulated block (blocking
not enabled) AlertDateTime: 16:52:17 2013-02-07 ObjectType: Target Port SourceAddress:
100.0.0.216 SensorAddress: 192.168.64.15"
```

Indegy Security Platform

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog (CEF formatted)	Host name and Device Type from LOG	Over 14 types of security logs	Security and Compliance

Event Types

Go to **ADMIN > Device Support > Event Types** and search for “Indegy-”.

Rules

None

Reports

None

Configuration

Configure Indegy Security Platform to send syslog in the supported format to FortiSIEM. No configuration is required in FortiSIEM.

Sample Events

```
<12>Nov 17 09:04:06 10.100.20.40 CEF:0|Indegy|Indegy Security
Platform|3.0.33|109|Unauthorized Conversation|7|dvchost=indegy rt=Nov 17 2019 09:04:06
duser=AS_01,Comm. Adapter #2 suser=Eng. Station #9 proto=UDP externalId=125
dst=10.100.102.150 src=10.100.20.34 dpt=47808 cs6Label=policy_name cs6=Use of Unauthorized
Protocols in Siemens Controllers cat=NetworkEvents
```

Juniper DDoS Secure

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		DDoS Alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "juniper-ddos" to see the event types associated with this device.

- Juniper-DDoS-Secure-WorstOffender
- Juniper-DDoS-Secure-Blacklisted
- Juniper-DDoS-Secure-Generic

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure the device to send syslog to FortiSIEM. Make sure that the event matches the format specified below.

```
<134>Juniper: End : 117.217.141.32 : IND: Worst Offender: Last Defended 66.145.37.254: TCP
Attack - Port Scan (Peak 55/s, Occurred 554)
<134>Juniper: End : 78.143.172.52 : IRL: IP Address Temp Black-Listed (Valid IP) Exceeds SYN
+ RST + F2D Count (Peak 114/s, Dropped 83.5K pkts)
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Juniper DDos Secure
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Juniper Networks IDP Series

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "juniper_idp" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog from NSM

```
<25>Oct 11 14:29:27 10.146.68.68 20101011, 58420089, 2010/10/11 18:29:25, 2010/10/11
18:33:12, global.IDP, 1631, par-real-idp200, 10.146.68.73, traffic, udp port scan in
progress, (NULL), (NULL), 161.178.223.221, 0, 0.0.0.0, 0, (NULL), (NULL), 10.248.8.110,
0, 0.0.0.0, 0, udp, global.IDP, 1631, Metro IDP IP / Port Scan Policy, traffic
anomalies, 2, accepted, info, yes, 'interface=eth3', (NULL), (NULL), (NULL), 0, 0, 0,
0, 0, 0, 0, 0, no, 25, Not
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Juniper Netscreen IDP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

McAfee IntruShield

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Settings for Access Credentials
- Configuration
- Sample Parsed Syslog Message

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	McAfee Intrushield
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Configuration

Syslog

FortiSIEM handles custom syslog messages from McAfee Intrushield.

1. Log in to McAfee Intrushield Manager.
2. Create a customer syslog format with these fields:
   - AttackName
   - AttackTime
   - AttackSeverity
   - SourceIp
   - SourcePort
   - DestinationIp
   - DestinationPort
   - AlertId
   - AlertType
   - AttackId
   - AttackSignature
   - AttackConfidence
   - AdminDomain
   - SensorName:ASCDCIPS01
   - Interface
   - Category
   - SubCategory
   - Direction
   - ResultStatus
   - DetectionMechanism
   - ApplicationProtocol
   - NetworkProtocol
   - Relevance
3. Set the message format as a sequence of `Attribute:Value` pairs as in this example.

```
AttackName:$IV_ATTACK_NAME$,AttackTime:$IV_ATTACK_TIME$,AttackSeverity::$IV_ATTACK_
SEVERITY$,SourceIp:$IV_SOURCE_IP$,SourcePort:$IV_SOURCE_PORT$,
DestinationIp:$IV_DESTINATION_IP$,DistinationPort:$IV_DESTINATION_PORT$,AlertId:$IV_
ALERT_ID$,AlertType:$IV_ALERT_TYPE$,AttackId$IV_ATTACK_ID$,
AttackSignature:$IV_ATTACK_SIGNATURE$,AttackConfidence:$IV_ATTACK_
CONFIDENCE$,AdminDomain:$IV_ADMIN_DOMAIN$,SensorName:$IV_SENSOR_NAME$,
Interface:$IV_INTERFACE$,Category:$IV_CATEGORY$,SubCategory:$IV_SUB_
CATEGORY$,Direction:$IV_DIRECTION$,ResultStatus:$IV_RESULT_STATUS$,
DetectionMechanism:$IV_DETECTION_MECHANISM$,ApplicationProtocol:$IV_APPLICATION_
PROTOCOL$,NetworkProtocol:$IV_NETWORK_PROTOCOL$,Relevance:$IV_RELEVANCE$
```

4. Set FortiSIEM as the syslog recipient.

Sample Parsed Syslog Message

```
Mar 24 16:23:18 SyslogAlertForwarder: AttackName:Invalid Packets detected,AttackTime:2009-
03-24 16:23:17 EDT,AttackSeverity:Low,SourceIp:127.255.106.236,

SourcePort:N/A,DestinationIp:127.255.106.252,DistinationPort:N/A,AlertId:5260607647261334188
,AlertType:Signature,AttackId:

0x00009300,AttackSignature:N/A,
AttackConfidence:N/A,AdminDomain:ASC,SensorName:ASCDCIPS01,Interface:1A-
1B,Category:Exploit,SubCategory:protocol-violation,Direction:Outbound,
ResultStatus:May be
successful,DetectionMechanism:signature,ApplicationProtocol:N/A,NetworkProtocol:

N/A,Relevance:N/A,HostIsolationEndTime:N/A
```

McAfee Stonesoft IPS

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Network IPS alerts	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "stonesoft" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM processes events from this device via **CEF formatted syslog** sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	McAfee Stonesoft IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Example Syslog

```
<6>CEF:0|McAfee|IPS|5.4.3|70018|Connection_Allowed|0|spt=123 deviceExternalId=STP-NY-FOO01
node 1 dmac=84:B2:61:DC:E1:31 dst=169.132.200.3 cat=System Situations app=NTP (UDP) rt=Apr
08 2016 00:26:13 deviceFacility=Inspection act=Allow deviceOutboundInterface=Interface #5
deviceInboundInterface=Interface #4 proto=17 dpt=123 src=10.64.9.3 dvc=12.17.2.17
dvchost=12.17.2.17 smac=78:DA:6E:0D:FF:C0 cs1Label=RuleId cs1=2097152.6
```

Motorola AirDefense

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Wireless IDS logs	Security Monitoring

Event Types

About 33 event types covering various Wireless attack scenarios. In **ADMIN > Device Support > Event Types**, search for "Motorola-AirDefense" in the **Search...** field to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure the device to send logs to FortiSIEM. Make sure that the format is as follows.

```
Nov  8 18:48:00 Time=2014-10-29T05:39:00,Category=Rogue
Activity,CriticalityLevel=Severe,Desc=Rogue AP on Wired Network,device=00:22:cf:5d:ee:60
(00:22:cf:5d:ee:60),sensor=fc:0a:81:12:7b:4b(COMP-SENS302EA[a,b,g,n])
Nov 12 13:33:00 Time=2015-11-
12T08:47:00,Category=Exploits,CriticalityLevel=Critical,Desc=NAV Attack -
CTS,device=5c:0e:8b:cb:d5:40(5c:0e:8b:cb:d5:40),sensor=fc:0a:81:12:77:3f(COMP-SENS201EA
[a,b,g,n])
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Motorola AirDefense
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Nozomi

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuring Syslog on Nozomi

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog	Device type	Node detection, protocol information, network changes	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Nozomi" to see the event types associated with this device.

Rules

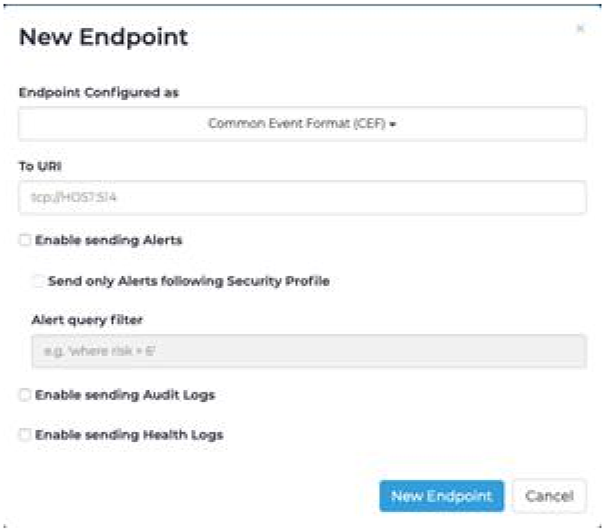
There are no specific rules for Nozomi, however rules that match the **Event Type Groups** associated with Nozomi Events may trigger.

Reports

There are no specific **Reports** for Nozomi, however reports that match the **Event Type Groups** associated with Nozomi Events may return results.

Configuring Syslog on Nozomi

1. Log in to the Guardian console.
2. Navigate to **Administration->Data Integration**.
3. Press **+Add** on the right side of the screen.
4. Select the **Common Event Format (CEF)** from the drop down.
5. You should see the data entry screen.



New Endpoint

Endpoint Configured as: Common Event Format (CEF)

To URI: tcp://HOST:514

□ Enable sending Alerts

□ Send only Alerts following Security Profile

Alert query filter: e.g. 'where risk > 6'

□ Enable sending Audit Logs

□ Enable sending Health Logs

6. Enter the appropriate host information. For example `udp://<FortiSIEM IP>:514`.
7. Select **Enable sending Alerts** and/or **Enable sending Audit Logs** and/or **Enable sending Health Logs**.
8. Press **New Endpoint**.

Palo Alto Cortex XDR

- Event Types
- Rules
- Reports
- Configuration

Event Types

In **ADMIN > Device Support > Event Types**, search for "cortexXDR" to see the event types associated with this device. In FortiSIEM 6.3.0, there are 9 event types for Cortex XDR.

Rules

In **RESOURCES > Rules**, search for "cortex" in the main content panel **Search...** field.

Reports

No specific reports are available for Palo Alto Cortex XDR.

Configuration

For the latest Palo Alto Cortex XDR documentation, see https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/logs/integrate-a-syslog-receiver-for-outbound-notifications.html.

Public or Self Signed Certificate Configuration

Fortinet recommends configuring Syslog over TLS for Cortex XDR.

You can generate either a public certificate or a self signed certificate.

- Public Certificate Generation and Application Configuration
- Self Signed Certificate Generation and Application Configuration

Prerequisites

- Ensure you have a collector that is publicly exposed (has a public IP with port TCP 6514 open).
- Be sure to specify a valid FQDN when registering the collector, and make sure a public DNS A record exists for it.
- Add a whitelist to restrict all traffic only from these destinations based on your region listed in the documentation here.

Public Certificate Generation and Application Configuration

Take the following steps:

1. Generate a SSL/TLS certificate using a public certificate. A public certificate can be signed by a public certificate authority (CA) such as DigiCert, or GoDaddy.
2. Run the following command on your collector to generate a CSR (Certificate Signing Request)

   ```
   cd /tmp
   openssl req -new -newkey rsa:4096 -nodes -keyout /etc/pki/tls/private/tls-collector1.key -out tls-collector1.csr
   ```
3. Take the following actions when prompted.
   a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
   b. Enter your State or Province. For example, California would be "CA".
   c. Enter your Locality. For example, a city would be "Sunnyvale".
   d. Enter your desired org name. For example, "Fortinet".
   e. Enter Unit Name, which is optional. For example, "IT".
   f. Enter Common Name. It must match the FQDN of collector. For example, "collector1.myorg.fortinet.com".
   g. Email Address. This can be left blank. Hit "enter" to continue.
   h. If prompted for a challenge password, hit "enter" to leave blank and continue.
   i. Hit enter again to confirm.
      A Certificate Signing Request is created in `/tmp/tls-collector1.csr`.
4. Using WinScp or another SCP utility, download this CSR file to your desktop.
5. Go to your preferred public CA, and upload this CSR when prompted to generate a new SSL certificate file.

   When you have your new Certificate ZIP file, it will normally contain 2-3 files.
6. WinSCP zip file to `/tmp` of the Collector.
7. Unzip the file if needed, by using the following command.

```
unzip <filename>.zip
```

The .crt file is your certificate, and is usually a concatenation of all chain certificates.

8. Rename the cert files if needed using similar commands here.

   ```
   cd /tmp
   mv 11111111.crt tls-collector1.crt
   ```

9. Copy the cert to the correct folder using the following command.

   ```
   cp tls-collector1.crt /etc/pki/tls/certs/tls-collector1.crt
   ```

10. Set permissions using the following command.

    ```
    chmod 644 /etc/pki/tls/certs/tls-collector1.crt
    chmod 640 /etc/pki/tls/private/tls-collector1.key
    chown root:admin /etc/pki/tls/private/tls-collector1.key
    ```

11. On the Collector, update the `/opt/phoenix/config/phoenix_config.txt` file to reference the new tls cert using the following command.

    ```
    vi /opt/phoenix/config/phoenix_config.txt
    ```

12. Locate the following lines in your `phoenix_config.txt` file.

    ```
    listen_tls_port_list=6514
    tls_certificate_file=/etc/pki/tls/certs/localhost.crt
    tls_key_file=/etc/pki/tls/private/localhost.key
    ```

    and replace the cert and key file with the following:

    ```
    listen_tls_port_list=6514
    tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt
    tls_key_file=/etc/pki/tls/private/tls-collector1.key
    ```

13. Save the file, and as root, restart phParser using the following command.

    ```
    killall -9 phParser
    ```

14. Define the Syslog server parameters (See step 4 in Integrate a Syslog Receiver for more information).
    - Name: FortiSIEM_Public_Collector
    - Destination: Pulbic IP or FQDN of FortiSIEM Collector
    - Port: 6514
    - Facility: Informational, or Default Value
    - Protocol: TCP + SSL/TLS
    - Certificate: You do not need to upload as it is a public signed SSL certificate.
15. Click **Create**.

Self Signed Certificate Generation and Application Configuration

Take the following steps:

1. On the Collector, run the following commands as root.

   ```
   cd /tmp
   openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 -keyout
   /etc/pki/tls/private/tls-collector1.key -out /etc/pki/tls/certs/tls-collector1.crt
   ```

2. Take the following actions when prompted.

   a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
   b. Enter your State or Province. For example, California would be "CA".
   c. Enter your Locality. For example, a city would be "Sunnyvale".
   d. Enter your desired org name. For example, "Fortinet".
   e. Enter Unit Name, which is optional. For example, "IT".
   f. Enter Common Name. It must match the FQDN of collector. For example, "collector1.myorg.fortinet.com".
   g. Email Address. This can be left blank. Hit "enter" to continue.
   h. If prompted for a challenge password, hit "enter" to leave blank and continue.
   i. Hit enter again to confirm.
3. Set the appropriate permissions for the private key and certificate generated, by running the following commands.

   ```
   chmod 640 /etc/pki/tls/private/tls-collector1.key
   chown root:admin /etc/pki/tls/private/tls-collector1.key
   chmod 644 /etc/pki/tls/certs/tls-collector1.crt
   ```
4. On the collector, update the `/opt/phoenix/config/phoenix_config.txt` file to reference the new tls certificate by editing the file, running the following command.

   ```
   vi /opt/phoenix/config/phoenix_config.txt
   ```
5. Find the following lines in the file.

   ```
   listen_tls_port_list=6514
   tls_certificate_file=/etc/pki/tls/certs/localhost.crt
   tls_key_file=/etc/pki/tls/private/localhost.key
   ```
   and replace the cert and key file with the following:

   ```
   listen_tls_port_list=6514
   tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt
   tls_key_file=/etc/pki/tls/private/tls-collector1.key
   ```
6. Save the file, and as root, restart phParser using the following command.

   ```
   killall -9 phParser
   ```
7. Make a copy of the certificate file to `/tmp`, and using WinSCP or another SCP utility, download the Collector Certificate file. For example, you may run the following command.

   ```
   cp /etc/pki/tls/certs/tls-collector1.crt /tmp
   ```
8. Download `/tmp/tls-collector1.crt` to your desktop.

   Note: You only need the Certificate file and not the private key. The private key will never leave the collector.
9. Define the Syslog server parameters (See step 4 in Integrate a Syslog Receiver for more information).
   - Name: FortiSIEM_Public_Collector
   - Destination: Pulbic IP or FQDN of FortiSIEM Collector
   - Port: 6514
   - Facility: Informational, or Default Value
   - Protocol: TCP + SSL/TLS
   - Certificate: You do not need to upload as it is a public signed SSL certifcate.
   - Select Ignore Certificate Error.
10. Click **Create**.

Radware DefensePro

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog		Over 120 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, Search for “Radware-DefensePro” in the main content panel **Search...** field to see the event types associated with this device.

Sample Event Type:

```
<132>DefensePro: 13-09-2017 15:03:21 WARNING 12572 Intrusions "SIP-Scanner-SIPVicious" UDP 1.1.1.1 29992 1.1.1.2 5060 15 Regular "GSN_Web" occur 1 3 N/A 0 N/A high drop FFFFFFFF-FFFF-FFFF-9C94-000F57F7595F
```

```
<132>DefensePro: 13-09-2017 15:18:45 WARNING 150 HttpFlood "HTTP Page Flood Attack" TCP 1.1.1.3 0 1.1.1.4 80 0 Regular "President-1.1.1.4" ongoing 100 0 N/A 0 N/A medium forward FFFFFFFF-FFFF-FFFF-9CCF-000F57F7595F
```

```
<132>DefensePro: 13-09-2017 14:37:53 WARNING 200000 SynFlood "SYN Flood HTTP" TCP 0.0.0.0 0 1.1.1.5 80 0 Regular "GSN_Web" ongoing 1 0 N/A 0 N/A medium challenge FFFFFFFF-FFFF-FFFF-9C46-000F57F7595F
```

```
<134>DefensePro: 13-09-2017 13:56:34 INFO Configuration Auditing manage syslog destinations create 172.16.10.207 -f "Local Use 0", ACTION: Create by user public via SNMP source IP 1.1.1.6
```

Rules

There are no specific rules but generic rules for Network IPS and Generic Servers apply.

Reports

There are no specific reports but generic rules for Network IPS and Generic Servers apply.

Configuration

Configure Radware DefensePro Security Manager to send syslog on port 514 to FortiSIEM.

Snort Intrusion Prevention System

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			
JDBC	**Generic information**: signature ID, signature name, sensor ID, event occur time, signature priority **TCP**: packet header, including source IP address, destination IP address, Source Port, Destination Port, TCP Sequence Number, TCP Ack Number, TCP Offset, TCP Reserved, TCP Flags, TCP Window size, TCP Checksum, tTCP Urgent Pointer; and packet payload **UDP**: packet header, including source IP address, destination IP address, Source Port, Destination Port, UDP Length, checksum; and packet payload **ICMP**: packet header, including source IP address, destination IP address, ICMP Type, ICMP Code, Checksum, ICMP ID, Sequence Number; and packet payload		
SNMP (for access to the database server hosting the Snort database)			

Event Types

In **ADMIN > Device Support > Event Types**, search for "snort-org" to see the event types associated with this device.

Configuration

Syslog

Collecting event information from Snort via syslog has two drawbacks:

1. It is not reliable because it is sent over UDP.
2. Information content is limited because of UDP packet size limit.

For these reasons, you should consider using JDBC to collect event information from Snort.

These instructions illustrate how to configure Snort on Linux to send syslog to FortiSIEM. For further information, you should consult the Snort product documentation.

1. Log in to your Linux server where Snort is installed.
2. Navigate to and open the file `/etc/snort/snort.conf`.
3. Modify `alert_syslog` to use a local log facility, for example:

   ```
    output alert_syslog: LOG_LOCAL4 LOG_ALERT
   ```

4. Navigate to and open the file `/etc/syslog.conf`.
5. Add a redirector to send syslog to FortiSIEM.

   ```
   #Snort log to local4
   #local4.*

   /var/log/snort.log
   #local4.*@192.168.20.41
   local4.alert@10.1.2.171
   ```

6. Restart the Snort daemon.

Example Parsed Snort Syslog

```
<161>snort[2242]: [1:206:9] BACKDOOR DeepThroat 3.1 CD ROM Open Client Request
[Classification: Misc activity] [Priority: 3]: {UDP} 192.168.19.1:6555 -> 172.16.2.5:514
<161>snort[5774]: [1:1560:6] WEB-MISC /doc/ access [Classification: access to a potentially
vulnerable web application] [Priority: 2]: {TCP} 192.168.20.53:41218 -> 192.168.0.26:80
<161>snort[5774]: [1:466:4] ICMP L3retriever Ping [Classification: Attempted Information
Leak] [Priority: 2]: {ICMP} 192.168.20.49 -> 192.168.0.10
<161>snort[5774]: [1:1417:9] SNMP request udp [Classification: Attempted Information Leak]
[Priority: 2]: {UDP} 192.168.20.40:1061 -> 192.168.20.2:161
```

JDBC

Supported Databases and Snort Database Schemas

When using JDBC to collect IPS information from Snort, FortiSIEM can capture a full packet that is detailed enough to recreate the packet via a PCAP file.

FortiSIEM supports collecting Snort event information over JDBC these database types:

- Oracle
- MS SQL

- MySql
- PostgreSQL

FortiSIEM supports Snort database schema 107 or higher.

SNMP Access to the Database Server

You must set up an SNMP access credential for the server that hosts the Snort database. See the topics under Database Server Configuration for information on setting up SNMP for communication with FortiSIEM for several common types of database servers.

Once you have set up SNMP on your database server, you can now configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Debugging Snort Database Connectivity

Snort IPS alert are pulled over JDBC by a Java agent, which has to join multiple database tables to create the events. An internal log file is created for each pull.

```
2012-08-07T10:02:27.576777+08:00 AO-foo java:[PH_JAVA_AGENT_INFO]:[eventSeverity]=PHL_INFO,
[procName]=phAgentManager,[fileName]=AgentSnort,[phLogDetail]=10.1.20.51:ICMP:Max record
id:17848444  Total records in one round of pulling:20
```

At most 1000 database records (IPS Alerts) are pulled at a time. If FortiSIEM finds more than 1000 new records, then it begins to fall behind and this log is created.

```
2012-08-07T10:02:27.576777+08:00 AO-foo java:[PH_JAVA_AGENT_INFO]:[eventSeverity]=PHL_INFO,
[procName]=phAgentManager,[fileName]=AgentSnort,[phLogDetail]=Event count of snort exceeds
the threshold in one round of pulling, which means there may be more events need to be
pulled.
```

Examples of Snort IPS Events Pulled over JDBC

- UDP Event
- TCP Event

UDP Event

```
<134>Feb 25 14:27:56 10.1.2.36 java: [Snort-1417]:[eventSeverity]=PHL_INFO,
[relayDevIpAddr]=10.1.2.36,[ipsSensorId]=1,[snortEventId]=10343430,
[sensorHostname]=10.1.2.36,[signatureId]=1417,[eventName]=SNMP request udp,
[eventSeverity]=2,[eventTime]=2012-11-07 17:56:51.0,[srcIpAddr]=10.1.2.245,
[destIpAddr]=10.1.2.36,[ipVersion]=4,[ipHeaderLength]=5,[tos]=0,[ipTotalLength]=75,[ipId]=0,
[ipFlags]=0,[ipFragOffset]=0,[ipTtl]=64,[ipProto]=17,[ipChecksum]=8584,[srcIpPort]=35876,
[destIpPort]=161,[udpLen]=55,[checksum]=39621,
[dataPayload]=302D02010104067075626C6963A520...
```

TCP Event

```
<134>Aug 08 09:30:59 10.1.20.51
java: [Snort-1000001]:[eventSeverity]=PHL_INFO,[hostIpAddr]=10.1.20.51,[sensorId]=1,
[eventId]=17897184,[signatureId]=1000001,[signatureName]=Snort
Alert [1:1000001:0],[signaturePri]=null,[eventTime]=2012-08-08
09:26:24.0,[srcIpAddr]=10.1.2.99,[destIpAddr]=10.1.20.51,[srcIpPort]=52314,[destIpPort]=80,
[seqNum]=967675661,[tcpAckNum]=3996354107,[tcpOffset]=5,[tcpReserved]=0,[tcpFlags]=24,
[tcpWin]=16695,[checksum]=57367,[tcpUrgentPointer]=0,
[dataPayload]=474554202F66617669636F6E2E69636F204...
```

Viewing Snort Packet Payloads in Reports

FortiSIEM creates an event for each IPS alert in Snort database. You can view the full payload packet associated with a Snort event when you run a report.

1. Set up a structured historical search.
2. Set these conditions, where **Reporting IP** is an IP belonging to the Snort Application group.

Attribute	Operator	Value
Reporting IP	IN	Applications: Network IPS App

3. For **Display Fields**, include **Data Payload**.
When you run the query, Data Payload will be one one of the display columns.
4. When the query runs, select an event, and the data payload will display at the bottom of the search results in a byte-by-byte ethereal/wireshark format.

Exporting Snort IPS Packets as a PCAP File

After running a report, click the **Export** button and choose the PCAP option.

Settings for Access Credentials

- Access Credentials for JDBC
- Access Credentials for SNMP, Telnet, SSH

Access Credentials for JDBC

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your Snort IPS over JDBC.

Setting	Value
Name	<database type>-snort-BT
Device Type	Select the type of database that you are connecting to for Snort alerts

Setting	Value
Access Protocol	JDBC
Used For	Snort Audit
Pull Interval (minutes)	1
Port	3306
Database Name	The name of the database
User Name	The administrative user for the Snort database
Password	The password associated with the administrative user

Access Credentials for SNMP, Telnet, SSH

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP, Telnet, or SSH.

Setting	Value
Name	<set name>
Device Type	Snort-org Snort IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sourcefire 3D and Defense Center

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "sourcefire" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- Syslog
- Sample Syslog from SourceFire3D IPS
- Sample Syslog from SourceFire Defense Center

Syslog

FortiSIEM handles SourceFire alerts via syslog either from IPS appliances themselves or from Defense Center. Events are classified as Snort event types.

Simply configure SourceFire appliances or Defense Center to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.

- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Sample Syslog from SourceFire3D IPS

```
<188>Jul  4 15:07:01 Sourcefire3D Snort: [119:15:1] http_inspect: OVERSIZE REQUEST-URI
DIRECTORY [Impact: Unknown] From DetectionEngine_IPS_DMZ2/SourcefireIPS at Thu Jul  4
15:07:01 2013 UTC [Classification: Potentially Bad Traffic] [Priority: 2] {tcp}
10.20.1.12:57689->1.1.1.1:80
```

Sample Syslog from SourceFire Defense Center

```
<46>Jul 17 16:01:54 DefenseCenter SFAppliance: [1:7070:14] "POLICY-OTHER script tag in URI -
likely cross-site scripting attempt" [Impact: Potentially Vulnerable] From "10.134.96.172"
at Wed Jul 17 16:01:52 2013 UTC [Classification: Web Application Attack] [Priority: 1] {tcp}
1.2.3.4:60537->2.3.4.5:80
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Sourcefire Sourcefire3D IPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Trend Micro Deep Discovery

- Integration Points
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

Integration Points

Method	Information discovered	Metrics collected	LOGs collected	Used for
Syslog	Host name, Reporting IP	None	Malicious file detection	Security monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Trend-DeepDiscoveryAnalyzer" and "Trend-DeepDiscoveryInspector" to see the event types associated with this device.

Rules

No specific rules are written for Trend Deep Discovery Analyzer and Trend Deep Discovery Inspector, but regular end point rules apply.

Reports

No specific reports are written for Trend Deep Discovery Analyzer and Trend Deep Discovery Inspector, but regular end point reports apply.

Configuration

Configure the Trend Deep Discovery system to send logs to FortiSIEM in the supported format (see Sample Events).

Settings for Access Credentials

None required.

Sample Events

```
<123>CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1175|20|Malware URL requested - Type
      1|6|
dvc=10.0.1.50 dvcmac=00:0C:29:A6:53:0C dvchost=ddi38-143
deviceExternalId=6B593E17AFB7-40FBBB28-A4CE-0462-A536 rt=Mar 09 2015 11:58:25 GMT+08:00
app=HTTP deviceDirection=1 dhost=www.example.com dst=10.10.11.99 dpt=80
dmac=00:1b:21:35:8b:98 shost=10.1.1.97 src=10.1.1.197 spt=12121 smac=fe:ed:be:ef:5a:c6
cs3Label=HostName_Ext cs3=www.example.com fname=setting.doc fileType=0 fsize=0 act=not
     blocked
cn3Label=Threat Type cn3=1 destinationTranslatedAddress=10.1.1.2
sourceTranslatedAddress=10.1.1.197 cnt=1 cs5Label=CCCA_DetectionSource
cs5=GLOBAL_INTELLIGENCE cn1Label=CCCA_Detection cn1=1 cat=Callback cs6Label=pAttackPhase
cs6=Command and Control Communication
```

Zeek (Bro) Installed on Security Onion (Legacy)

See Zeek Network Security Monitor (Previously known as Bro) for the latest information.

Bro/Zeek is an OpenSource network analysis product that is also installed as part of Security Onion.

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog			Event Collection

Event Types

- `Bro-dhcp /Regular Traffic/Permit` - Traffic A DHCP conversation
- `Bro-dns /Regular Traffic/Permit` - Traffic DNS activity log
- `Bro-conn /Regular Traffic/Permit` - Traffic TCP/UDP/ICMP connections
- `Bro-app_stats /Info` - Statistics about APP
- `Bro-radius /Info` - RADIUS analysis activity
- `Bro-known_devices /Info` - Bro known devices

Rules

Generic Rules matching categories.

Reports

Generic Reports matching categories.

Configuration

Complete the following task on Onion Security, as this is crucial to get the headers working in the parser:

Add the following code in the `/etc/syslog-ng/syslog-ng.conf` file, but change *<IP>* to the IP of the FortiSIEM Super/Worker/Collector which will receive the syslog:

```
destination d_fortisiem { tcp("<IP>" port(514));};
log {
source(s_bro_dns);
source(s_bro_dhcp);
log { filter(f_bro_headers); };
log { destination(d_fortisiem);};
};
```

Sample Events

```
<13>Mar 25 11:02:24 sec-sensor-ps bro_dns: {"ts":"2019-03-
25T11:02:22.485187Z","uid":"CEBf4c2FoLEBtbPLn6","id.orig_h":"10.8.20.21","id.orig_
p":50837,"id.resp_h":"10.8.1.203","id.resp_p":53,"proto":"udp","trans_
id":25959,"rtt":0.000357,"query":"tsomething.my.somewhere.com","qclass":1,"qclass_name":"C_
INTERNET","qtype":1,"qtype_name":"A","rcode":0,"rcode_
name":"NOERROR","AA":false,"TC":false,"RD":true,"RA":true,"Z":0,"answers":["um1.my.
somewhere.com","um1-lo3.my. somewhere.com","um1-lo3.lo3.r.my.
somewhere.com","55.66.8.24","55.66.8.152","55.66.9.24"],"TTLs":
[136.0,5.0,146.0,5.0,5.0,5.0],"rejected":false}
```

Operational Technology

FortiSIEM supports these operational technology applications/devices for discovery and monitoring.

- APC Netbotz Environmental Monitor
- APC UPS
- Claroty Continuous Threat Detection
- CyberX OT/IoT Security
  Dragos Platform
- Generic UPS
- Hirschmann SCADA Firewalls and Switches
- Liberty FPC
- Liberty HVAC
- Liberty UPS
- Nozomi
- Otorio RAM2 (Risk Assessment, Monitoring and Management)

APC Netbotz Environmental Monitor

- What is Monitored and Collected
- Event Types
- Rules
- Reports
- Configuration
- Setting Access Credentials

What is Monitored and Collected

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	**Temperature**: Sensor Id, Sensor label, Enclosure Id, Temperature **Relative Humidity**: Sensor Id, Sensor label, Enclosure Id, Relative Humidity **Air Flow**: Sensor Id, Sensor label, Enclosure Id, Air Flow **Dew Point Temperature**: Sensor Id, Sensor label, Enclosure Id, Dew Point Temperature **Current**: Sensor Id, Sensor label, Enclosure Id, Current **Audio Sensor Reading**: Sensor Id, Sensor label, Enclosure Id, Audio Sensor Reading **Dry Contact Sensor Reading**: Sensor Id, Sensor label, Enclosure Id, Dry Contact Sensor Reading	Availability and Performance Monitoring
		Door Switch Sensor Reading: Sensor Id, Sensor label, Enclosure Id, Door Switch Sensor Reading (Open/Close) **Camera Motion Sensor Reading**: Sensor Id, Sensor label, Enclosure Id, Camera Motion Sensor Reading (Motion/No Motion) **Hadware Status (for NBRK0200)**: Contact Status, Output Relay Status, Outlet Status, Alarm Device Status, Memory Sensor Status, Memory Output Status, Memory Outlet Status, memory Beacon Status **EMS Status (for NBRK0200)**: EMS Hardware Status, Connection State **Hardware Probe (for NBRK0200)**: Sensor Id, Temperature, Relative Humidity, Connection State Code **Module Sensor (for NBRK0200)**: Sensor Name, Sensor location, Temperature, Relative Humidity, Connection State Code	
SNMP Trap (V1, V2c)	SNMP Trap	See **Event Types** for more information about viewing the SNMP traps collected by FortiSIEM for this device.	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "NetBotz" to see the event types associated with this application or device.

Event types for NetBotz NBRK0200

- PH_DEV_MON_HW_STATUS

```
[PH_DEV_MON_HW_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,
[lineNumber]=1642,[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[hwStatusCode]=2,
[hwProbeStatus]=2,[hwInputContactStatus]=2,[hwOutputRelayStatus]=0,[hwOutletStatus]=2,
[hwAlarmDeviceStatus]=0,[hwMemSensorStatus]=0,[hwMemOutputStatus]=2,
[hwMemOutletStatus]=2,[hwMemBeaconStatus]=2,[phLogDetail]=
```

- PH_DEV_MON_HW_EMS_STATUS

```
[PH_DEV_MON_HW_EMS_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,
[lineNumber]=1871,[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[reptDevName]=Unknown,
[emsHwStatus]=0,[phyMachConnectionStateCode]=2,[hwLogStatus]=1,[phLogDetail]=
```

- PH_DEV_MON_HW_PROBE

```
[PH_DEV_MON_HW_PROBE]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,
[lineNumber]=2100,[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[envSensorLabel]=Sensor
MM:4,[envTempDegF]=74,[envTempHighThreshDegF]=138,[envHumidityRel]=51,
[envHumidityRelHighThresh]=90,[envHumidityRelLowThresh]=10,[serialNumber]=L3,
[phyMachConnectionStateCode]=3,[maxTempThresh]=140,[minTempThresh]=32,
[maxHumidityThresh]=99,[minHumidityThresh]=0,[phLogDetail]=
```

- PH_DEV_MON_HW_MODULE_SENSOR

```
[PH_DEV_MON_HW_MODULE_SENSOR]:[eventSeverity]=PHL_INFO,[fileName]=deviceNetBotz.cpp,
[lineNumber]=2567,[hostName]=Unknown,[hostIpAddr]=10.62.97.61,[moduleNumber]=0,
[envSensorId]=1,[envSensorLabel]=Sensor MM:1,[envSensorLoc]=Orland Park Server,
[envTempDegF]=74,[envHumidityRel]=50,[phyMachConnectionStateCode]=1,
[hwAlarmDevicetatus]=1,[phLogDetail]=
```

Rules

In **RESOURCES > Rules**, search for "NetBotz" in the main content panel **Search...** field to see the rules associated with this application or device.

Reports

In **RESOURCES > Reports**, search for "NetBotz" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Setting Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	APC NetBotz
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

APC UPS

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	**UPS metrics**: Remaining battery charge, Battery status, Replace battery indicator, Time on battery, Output status, Output load, Output voltage, Output frequency	Availability and Performance Monitoring
SNMP Trap			Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "apc" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "apc" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "apc" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Setting Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	APC UPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Claroty Continuous Threat Detection (CTD) Platform

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Claroty Alert, Baseline and Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "ClarotyCTD" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 20 event types defined.

Rules

There are no specific rules available for Claroty.

Reports

There are no specific reports available for Claroty. You can view all Claroty events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "ClarotyCTD".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<12>Sep 12 15:31:33 localhost.localdomain
CEF:0|Claroty|CTD|2.7.0|Baseline|None|Unapproved|cs1Label=Site cs1=Site cs2Label=Network
cs2=Default cs3Label=Transmission cs3=TCP / 44818 cs4Label=SiteId cs4=1 cs5Label=SrcZone
cs5=Engineering Station: Rockwell cs6Label=DstZone cs6=PLC: Rockwell cs7Label=Category
cs7=Protocol cs8Label=CategoryAccess cs8=Read cs9Label=Frequency cs9=NotTimed
cs10Label=FirstSeen cs10=Sep 12 2018 15:31:29 src=10.1.30.40 smac=00:50:56:b9:e2:ad
shost=N/A dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d dhost=N/A externalId=2365 cat=Create rt=Sep
12 2018 15:31:29 msg=CIP : Service Get Attribute All called on ExtendedDevice


<12>Sep 12 15:18:03 localhost.localdomain CEF:0|Claroty|CTD|2.7.0|Alert|Configuration
Download|Critical|cs1Label=Site cs1=Site cs2Label=Network cs2=Default cs3Label=ResolvedAs
cs3=Unresolved cs4Label=SiteId cs4=1 cs5Label=SrcZone cs5=Engineering Station: Rockwell
cs6Label=DstZone cs6=PLC: Rockwell cs7Label=Category cs7=Integrity cs8Label=AlertUrl
cs8=https://10.210.16.2:5000/alert/74-1 src=10.1.30.40 smac=00:50:56:b9:e2:ad shost=N/A
dst=10.1.30.1 dmac=00:1d:9c:c0:04:9d dhost=N/A externalId=74 cat=Create rt=Sep 12 2018
15:18:01 msg=A configuration has been downloaded to controller Chemical_plant by 10.1.30.40
```

CyberX OT/IoT Security

- Event Types
- Rules
- Reports
- Configuration

Event Types

In **ADMIN > Device Support > Event Types**, search for "cyberx" to see the event types associated with this device. In FortiSIEM 6.3.0, there are 5 event types defined.

Rules

In FortiSIEM 6.3.0, CyberX Security Alerts and CyberX Malware Detected are available.

Reports

In 6.3.0, a CyberX Security Alerts report is available.

Configuration

- Syslog Configuration

Syslog Configuration

For the latest CyberX documentation, see https://cyberx-labs.zendesk.com/hc/en-us/articles/360009152892-How-To-Create-Forwarding-Rules.

To configure syslog, take the following steps:

1. Login to the CyberX Platform UI.
2. In the left menu, go to the **Forwarding** menu.
3. Create a new forwarding rule.
4. In the **Name** field, enter "FortiSIEM_Notification" or your desired name.
5. For **Protocols**, select **All**.
6. For **Engines**, select **All**.
7. Select the Informational Severity option for your desired severity level.
8. Under **Actions**, click **Add**.
9. Select **Send to SYSLOG Server (CEF Format)**.
10. In the **Host** field, enter the IP or hostname of your FortiSIEM collector.
11. In the **Port** field, enter "514".
12. In the **Timezone** field, enter your timezone.
13. Click **Submit** when done.

Dragos Platform

- What is Discovered and Monitored
- Event Types
- Rules
- Reports

- Configuration
- Sample Syslog

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Dragos Alert logs regarding Modeling, Indicator, Configuration, Threat Behavior	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "dragos" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 5 event types defined.

Rules

There are no specific rules available for Dragos.

Reports

There are no specific reports available for Dragos.

There are no specific reports available for Dragos. You can view all Dragos events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Dragos".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

Sample Syslog

```
<13>1 2020-07-02T14:58:31.538019Z dragos dragos_syslog - - system="Dragos Platform"
createdAt="2020-07-02T14:58:31Z" summary="Test Message from Dragos App" severity="
{severity}" content="This test message was created by the Dragos Syslog App" asset_ip=#"
{asset_ip}" asset_hostname="Test" dst_asset_ip="10.0.0.9" dst_asset_hostname="Test" dst_
asset_mac="83:77:DB:E3:A3:38" dst_asset_domain="ip-10-10-255-1.ec2.test" src_asset_
ip="10.0.0.9" src_asset_hostname="Test" src_asset_mac="89:3A:EE:01:0F:D3" src_asset_
domain="ip-10-10-test.ec2.test" id="1234567" asset_domain="ip-10-10-255-1.ec2.test" asset_
id="111111" asset_mac="06:92:1C:1B:F2:72" detection_quad="Modeling" detectorId="test-
detector-1111" dst_asset_id="333333" matchedRuleId="16" occurredAt="2020-07-02T14:58:31Z"
originalSeverity="0" reviewed="False" src_asset_id="222222" type="Test"
```

```
<8>May 06 21:06:19 dragos dragos_syslog: CEF:0|Dragos|Platform|1.6|notification|Test Message
from Dragos App|5|content=This test message was created by the Dragos Syslog App asset_
ip=10.0.0.9 asset_hostname=Test dst_asset_ip=10.0.0.9 dst_asset_hostname=Test dst_asset_
mac=9C:B6:TE:ST:4B:95 dst_asset_domain=ip-10-10-255-1.ec2.test src_asset_ip=10.0.0.9 src_
asset_hostname=Test src_asset_mac=TE:ST:D0:F2:4B:95 src_asset_domain=ip-10-10-test.ec2.test
id=1234567 asset_domain=ip-10-10-255-1.ec2.test asset_id=111111 asset_mac=9C:B6:D0:F2:TE:ST
createdAt=2020-05-06T21:06:24Z detection_quad=Indicator detectorId=test-detector-4444 dst_
asset_id=333333 matchedRuleId=16 occurredAt=2020-05-06T21:06:24Z originalSeverity=5
reviewed=False src_asset_id=222222 type=Test
```

Generic UPS

- What is Discovered and Monitored
- Configuration
- Setting Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	**UPS metrics**: Remaining battery charge, Battery status, Time on battery, Estimated Seconds Remaining, Output voltage, Output current, Temperature	Availability and Performance Monitoring

Configuration

SNMP

Note: UPS-MIB Required

Your device must have a UPS-MIB database to communicate with FortiSIEM over SNMP.

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation, then follow the instructions in "Discovery Settings" and "Setting Credentials" in the User Guide, to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Setting Access Credentials

SNMP Access Credentials for All Devices

Use these **Access Method Definition** settings to allow FortiSIEM to access your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Hirschmann SCADA Firewalls and Switches

- What is Discovered and Monitored
- Event Types

- Rules
- Reports
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
SNMP	Host Name	SNMP – Uptime, CPU, Memory, Interface utilization, hardware Status, OSPF metrics	Performance Monitoring

Event Types

The following event types are used for performance monitoring:

- `PH_DEV_MON_SYS_UPTIME` - Uptime monitoring
- `PH_DEV_MON_SYS_CPU_UTIL` – CPU utilization
- `PH_DEV_MON_SYS_MEM_UTIL` – Memory utilization
- `PH_DEV_MON_NET_INTF_UTIL` – Interface utilization
- `PH_DEV_MON_HW_STATUS` – Hardware status

Rules

All performance monitoring rules apply.

Reports

All performance monitoring reports apply.

Configuration

Configure Hirschmann firewalls and switches for SNMP V1/V2c/V3 discovery and performance monitoring. Define the basic SNMP credentials on FortiSIEM and discover these devices. See SNMP Access Credentials.

Sample Events

The events are standard for all devices.

Liebert FPC

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	Output voltage (X-N, Y-N, Z-N), Output current (X, Y. Z), Neutral Current, Ground current, Output power, Power Factor, Output Frequency, Output Voltage THD (Vx, Vy, Vz), Output Current THD (Lx, Ly. Lz), Output KWh, Output Crest factor (Lx, Ly, Lz), Output K-factor (Lx, Ly, Lz), Output Lx Capacity, output Ly capacity	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Liebert FPC" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "Liebert FPC" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Liebert FPC
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Liebert HVAC

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	**HVAC metrics**: Temperature: current value, upper threshold, lower threshold, Relative Humidity: current value, upper threshold, lower threshold, System state, Cooling state, Heating state, Humidifying state, Dehumidifying state, Economic cycle, Fan state, Heating capacity, Cooling capacity	Availability and Performance Monitoring

FortiSIEM uses SNMP to discover and collector metrics from Generic UPS devices. This requires the presence of UPS-MIB on the UPS device.

See the Liebert HVAC documentation to enable FortiSIEM to poll the device via SNMP.

Event Types

In **ADMIN > Device Support > Event Types**, search for "Liebert HVAC" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports** , search for "Liebert HVAC" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

Note: UPS-MIB Required

Your device must have a UPS-MIB database to communicate with FortiSIEM.

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Liebert HVAC
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Access Credentials

Liebert UPS

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Hardware model, Network interfaces	**UPS metrics**: Remaining battery charge, Battery status, Time on battery, Estimated Seconds Remaining, Output voltage, Output current, Temperature	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

Note: UPS-MIB Required

Your device must include a UPS-MIB database to communicate with FortiSIEM.

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your device.

Setting	Value
Name	<set name>
Device Type	Liebert UPS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Nozomi

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuring Syslog on Nozomi

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog	Device type	Node detection, protocol information, network changes	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Nozomi" to see the event types associated with this device.

Rules

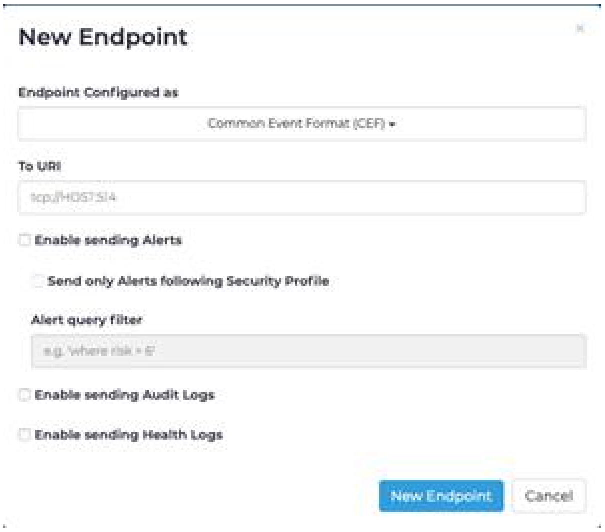
There are no specific rules for Nozomi, however rules that match the **Event Type Groups** associated with Nozomi Events may trigger.

Reports

There are no specific **Reports** for Nozomi, however reports that match the **Event Type Groups** associated with Nozomi Events may return results.

Configuring Syslog on Nozomi

1. Log in to the Guardian console.
2. Navigate to **Administration->Data Integration**.
3. Press **+Add** on the right side of the screen.
4. Select the **Common Event Format (CEF)** from the drop down.
5. You should see the data entry screen.



New Endpoint

Endpoint Configured as

Common Event Format (CEF) ▾

To URI

tcp://HOST:514

☐ Enable sending Alerts

☐ Send only Alerts following Security Profile

Alert query filter

e.g. 'where risk > 6'

☐ Enable sending Audit Logs

☐ Enable sending Health Logs

6. Enter the appropriate host information. For example `udp://<FortiSIEM IP>:514`.
7. Select **Enable sending Alerts** and/or **Enable sending Audit Logs** and/or **Enable sending Health Logs**.
8. Press **New Endpoint**.

Otorio RAM2 (Risk Assessment, Monitoring and Management)

FortiSIEM Supported added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Otorio

Product Information: https://www.otorio.com/resources/ram2-next-generation-ot-soar/

- Log Information
- Event Types
- Rules
- Reports

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for Otorio" to see the event types associated with this device. In FortiSIEM 6.3.1, there are 12 event types defined.

Rules

In **RESOURCES > Rules**, search for "Otorio" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 rules available.

- Otorio RAM2 Alert has Triggered
- Otorio RAM2 Vulnerability Discovered

Reports

In **RESOURCES > Reports**, search for "Otorio" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 2 reports available.

- Otorio RAM2 Alerts
- Otorio RAM2 Vulnerabilities Discovered

Routers and Switches

FortiSIEM supports these routers and switches for discovery and monitoring.

- Alcatel TiMOS and AOS Switch
- Arista Router and Switch
- ArubaOS-CX Switching Platform
- Brocade NetIron CER Routers
- Cisco 300 Series Routers
- Cisco IOS Router and Switch
    - How CPU and Memory Utilization is Collected for Cisco IOS
- Cisco Meraki Cloud Controller and Network Devices
- Cisco NX-OS Router and Switch
- Cisco ONS
- Cisco Viptela SDWAN Router
- Dell Force10 Router and Switch
- Dell N-Series Switch
- Dell PowerConnect Switch and Router
- Foundry Networks IronWare Router and Switch
- HP/3Com ComWare Switch
- HP ProCurve Switch
- HP Value Series (19xx) and HP 3Com (29xx) Switch
- Hirschmann SCADA Firewalls and Switches
- Juniper Networks JunOS Switch
- MikroTik Router
- Nortel ERS and Passport Switch

Alcatel TiMOS and AOS Switch

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Software version, Hardware model, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c)		Hardware status: Power Supply, Fan, Temperature	Availability
SNMP (V1, V2c, V3)	Layer 2 port mapping: associating switch ports to directly connected host IP/MAC addresses		Identity and location table; Topology

Event Types

In **ADMIN > Device Support > Event Types**, search for "alcatel" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Arista Router and Switch

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial number, Software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), CPU utilization, Memory utilization, Flash utilization, Hardware Status	Availability and Performance Monitoring
Telnet/SSH	Running and Startup configurations	Startup Configuration Change, Difference between Running and Startup configurations	Change monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- Telnet/SSH
- SNMP

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

- `show startup-config`
- `show running-config`
- `show version`
- `show ip route`
- `enable`
- `terminal pager 0`

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet

Setting	Value
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

ArubaOS-CX Switching Platform

FortiSIEM Support added: 6.3.2

Vendor: Aruba Networks (a Hewlett Packard Enterprise company)

Product Information: https://www.arubanetworks.com/products/switches/

- What is Discovered and Monitored
- Configuration
- Sample Events

What is Discovered and Monitored

The following protocols are used to discover and monitor various aspects of ArubaOS-CX switches.

Protocol	Metrics Collected	Used For
Syslog	Audit logs, General Performance and Availability logs	Security and Compliance

Configuration

Logging allows you to add syslog servers where the event log messages related to the AOS-CX switches are saved. For each of the syslog server added, you can configure the severity of the event logs to be saved on these servers. Configuration of the severity level for the debug logs can be done by configuring the severity at the global level. However, a minimum of one syslog server must be added to configure the global severity level.

- Configuration via CLI
- Configuration via GUI

Configuration via CLI

To configure syslog for an ArubaOS-CX switch, run the following CLI command.

```
logging <destIP or FQDN of FortiSIEM collector>
```

Example: logging 192.0.2.0

Configuration via GUI

To configure syslog for an ArubaOS-CX switch, take the following steps.

Note: For the latest configuration instructions, see **Configuring Logging Servers for AOX-CX** at https://help.central.arubanetworks.com/latest/documentation/online_help/content/aos-cx/cfg/conf-cx-logging.htm

1. In the **Network Operations** app, select one of the following options:
   a. To select a group in the filter:
      i. Set the filter to a group. The dashboard context for the group is displayed.
      ii. Under **Manage**, click **Devices > Switches**.
      iii. Click the **AOS-CX** or the **Config** icon to view the AOS-CX switch configuration dashboard.
   b. To select a switch:
      i. Set the filter to **Global** or a group containing at least one switch.
      ii. Under **Manage**, click **Devices > Switches**. A list of switches is displayed in the List view.
      iii. Click an AOS-CX switch under **Device Name**. The dashboard context for the switch is displayed.
      iv. Under **Manage**, click **Device**.
      The AOS-CX UI configuration page is displayed.
2. Click **System > Logging**. The Logging page is displayed.
3. Select the debug syslog severity level at the global level from the **Level** drop-down list.This severity level is applied to the debug logs that are saved on the syslog servers. You must add a minimum of one event syslog server before configuring the global severity level.
4. In the **Logging Servers** table, click **+** to add a logging server and configure the following parameters in the Add Logging Server page.

Parameters	Description	Value
FQDN or IP address	Fully Qualified Domain Name (FQDN) hostname	Enter the IPv4

Parameters	Description	Value
	or IP address of the logging server.	address in the x.x.x.x format or the hostname of the server.
Level	Severity level of the events that the logging server must log.	The following severity levels are supported: • Emergency • Critical • Alert • Error • Warning • Notice • Information • Debug
VRF	VRF on which the logging server is configured.	**Default** or **Management**.

5. Click **Apply** and then click **Save**.
6. To edit parameters of a logging server, select the row in the **Logging Servers** table and click the edit icon. The Edit Logging Server page is displayed. You can edit only the event log severity level and the VRF.
7. Click **Apply** and then click **Save**.
8. To delete the syslog server, select the row in the **Logging Servers** table and click the delete icon.
9. Click **OK** in the confirmation pop-up and then click **Save**.

Sample Events

```
<190>1 2021-08-31T12:29:06.148824-06:00 lab-1 hpe-restd 886 - - Event|4604|LOG_INFO|AMM|-
|Session started for user user1, session reO7LY123452GW7JlMw==
<190>1 2021-09-01T07:43:56.409226-06:00 lab-1 hpe-restd 886 - - Event|4609|LOG_INFO|AMM|-
|User aruba-admin added newuser-test with role admin-role
```

Brocade NetIron CER Routers

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces	CPU, Memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware Status, Real Server Status	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules specifically for this device.

Reports

There are no predefined reports specifically for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Brocade NetIron CER
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco 300 Series Routers

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces	Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards, and queue lengths)	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules specifically for this device.

Reports

There are no predefined reports specifically for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Cisco IOS Router and Switch

Issue with Generic Serial Numbers in Older Versions of Cisco IOS Routers

FortiSIEM uses serial numbers to uniquely identify a device. For older routers, the serial number is obtained from the OID `1.3.6.1.4.1.9.3.6.3.0`. However, this value is often incorrectly set by default to a generic value like `MSFC 2A`. If multiple routers have a common default value, then these routers will be merged into a single entry in the FortiSIEM CMDB.

You can check the current value for the serial number in a Cisco router by doing a SNMP walk of the OID.

```
snmpwalk -v2c -c <cred> <ip> 1.3.6.1.4.1.9.3.6.3.0
```

If the value is a generic value, then set it to the actual serial number.

```
Router(config)#snmp-server chassis-id
 Router(config)#exit
 Router#write memory
```

Run the snmpwalk again to verify that the serial number is updated, then perform discovery of your Cisco router.

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	Host name, IOS version, Hardware model, Memory size, Network interface details - name, address, mask and description	Uptime, CPU and Memory utilization, Free processor and I/O memory, Free contiguous processor and I/O memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths),	Availability and Performance Monitoring
SNMP (V1, V2c, V3)	Hardware component details: serial number, model, manufacturer, software firmware versions of hardware components such as chassis, CPU,	Hardware health: temperature, fan and power supply	Availability

Protocol	Information Discovered	Metrics collected	Used for
	fan, power supply, network cards etc.		
SNMP (V1, V2c, V3)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location
SNMP (V1, V2c, V3)	BGP connectivity, neighbors, state, AS number	BGP state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)	OSPF connectivity, neighbors, state, OSPF Area	OSPF state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)		**IP SLA and VoIP performance metrics:** Max/Min/Avg Delay and Jitter - both overall and Source->Destination and Destination->Source, Packets Lost - both overall and Source->Destination and Destination->Source, Packets Missing in Action, Packets Late, Packets out of sequence, VoIP Mean Opinion Score (MOS), VoIP Calculated Planning Impairment Factor (ICPIF) score	VoIP Performance Monitoring
SNMP (V1, V2c, V3)		**Class based QoS metrics** (from CISCO-CLASS-BASED-QOS-MIB): For (router interface, policy, class map) tuple: **class map metrics** including Pre-policy rate, post-police rate, drop rate and drop pct; **police action metrics** including conform rate, exceeded rate and violated rate; **queue metrics** including current queue length, max queue length and discarded packets	QoS performance monitoring
SNMP (V1, V2c, V3)		**NBAR metrics** (from CISCO-NBAR-PROTOCOL-DISCOVERY-MIB): For each interface and application, sent/receive flows, sent/receive bytes, sent/receive bits/sec	Performance Monitoring
Telnet/SSH	Running and startup configuration, Image file name,	Startup configuration change, delta between running and startup configuration, Running process CPU and memory utilization	Performance Monitoring, Security and

Protocol	Information Discovered	Metrics collected	Used for
	Flash memory size, Running processes		Compliance
Syslog	Device type	System logs and traffic logs matching acl statements	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco_ios" to see the event types associated with this device.

Configuration

- Telnet/SSH
- SNMP
- Syslog
- NetFlow
- IP SLA
- Class-Based QoS
- NBAR

Telnet/SSH

FortiSIEM uses SSH and Telnet to communicate with your device. Follow the instructions in the product documentation for your device to enable SSH and Telnet.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

- `show startup-config`
- `show running-config`
- `show version`
- `show flash`
- `show ip route`
- `show mac-address-table or show mac address-table`
- `show vlan brief`
- `show process cpu`
- `show process mem`
- `show disk0`
- `enable`
- `terminal pager 0`

SNMP

SNMP V1/V2c

1. Log in to the Cisco IOS console or telnet to the device.
2. Enter configuration mode.
3. Create an access list for FortiSIEM.

   ```
   access-list 10 permit <FortiSIEM IP>
   ```

4. Set up community strings and access lists.

   ```
   snmp-server community <community string> ro 10
   ```

5. Exit configuration mode.

SNMP V3

1. Log in to the Cisco IOS console or telnet to the device.
2. Enter configuration mode.
3. Create an access list for FortiSIEM.

   ```
   access-list 10 permit <FortiSIEM IP>
   ```

4. Set up SNMP credentials for Authentication only.

   ```
   snmp-server group <grpName> v3 auth
   #do this for every VLAN for FortiSIEM to discover per VLAN information such Spanning
   Tree and VTP MIBs
   snmp-server group <grpName> v3 auth context vlan-<vlanId>snmp-server user <userName>
   <grpName> v3 auth md5 <password> access 10
   ```

5. Set up SNMP credentials for Authentication and Encryption.

   ```
   snmp-server group <grpName> v3 priv
   #do this for every VLAN for FortiSIEM to discover per VLAN information such Spanning
   Tree and VTP MIBs
   snmp-server group <grpName> v3 auth context vlan-<vlanId>snmp-server group <grpName> v3
   priv context vlan-<vlanId>snmp-server user <userName> <grpName> v3 auth md5 <password>
   priv des56 <password> access 10
   ```

6. Exit configuration mode.

Additional IOS SNMPv3 Configuration Examples

IOS

```
enable
```

```
config t
```

```
snmp-server contact "contact info"
```

```
snmp-server location "location info"
```

```
snmp-server group fsiem_group v3 priv
```

```
#Note, check the context sensitive help in your IOS version to see if aes 128 is
supported instead of des56.

snmp-server user fortisiem_user fsiem_group 192.168.1.2 v3 auth sha "yourShaPassword"
priv des56 "yourDesPassword"

copy running-config startup-config
```

IOS XE

```
enable

config t

snmp-server group fsiem_group v3 priv

snmp-server user fortisiem fsiem_group 192.168.1.2 v3 auth sha "yourShaPassword" priv
aes 128 "yourAesPassword"

copy running-config startup-config
```

IOS XR

```
#Note not all models running IOS XR can support aes 128, some may only support des

configure

snmp-server contact "contact info"

snmp-server location "location info"

snmp-server group fsiem_group v3 priv

snmp-server user fortisiem fsiem_group v3 auth sha "yourShaPassword" priv aes 128
"yourDesPassword"

commit
```

Nexus 9K

```
config t

snmp-server contact "contact info"

snmp-server location "location info"

snmp-server user fortisiem auth sha "yourShaPassword" priv aes-128 "yourAesPassword"

snmp-server user fortisiem enforcePriv

copy running-config startup-config
```

Syslog

1. Login to the Cisco IOS console or telnet to the device.
2. Enter configuration mode.

3. Enable logging with these commands.

   ```
   logging on
   logging trap informational
   logging <FortiSIEM IP>
   ```

4. Make sure that the timestamp in syslog message sent to FortiSIEM does not contain milliseconds.

   ```
   no service timestamps log datetime msec
   service timestamps log datetime
   ```

5. To log traffic matching acl statements in stateless firewall scenarios, add the `log` keyword to the acl statements.

   ```
   access-list 102 deny udp any gt 0 any gt 0 log
   ```

6. To turn on logging from the IOS Firewall module, use this command.

   ```
   ip inspect audit-trail
   ```

7. Exit configuration mode.

Sample Cisco IOS Syslog Messages

```
<190>109219: Jan  9 18:03:35.281: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session: initiator
(192.168.20.33:1876) -- responder (192.168.0.10:445)

<190>263951: 2w6d: %SEC-6-IPACCESSLOGP: list permit-any permitted udp 192.168.20.35(0) ->
192.168.23.255(0), 1 packet

<188>84354: Dec  6 08:15:20: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: Admin] [Source:
192.168.135.125] [localport: 80] [Reason: Login Authentication Failed - BadPassword] at
08:15:20 PST Mon Dec 6 2010

<189>217: May 12 13:57:23.720: %SYS-5-CONFIG_I: Configured from console by vty1
(192.168.29.8)

<189>Oct 27 20:18:43.254 UTC: %SNMP-3-AUTHFAIL: Authentication failure for SNMP request from
host 192.168.2.98
```

NetFlow

Enable NetFlow on the Router

1. Enter configuration mode.
2. For **every interface**, run this command.

   ```
   interface <interface> <interface_number>ip route-cache flow
   exit
   ```

Set Up NetFlow Export

1. Enter configuration mode.
2. Run these commands.

```
ip flow-export version 5|9
ip flow-export destination <Accelops IP> 2055
ip flow-export source <interface> <interface_number>ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
```

On MLS switches, such as the 6500 or 7200 models, also run these commands.

```
mls netflow
mls nde sender
mls aging long 64
mls flow ip full
Exit configuration mode
```

You can verify that you have set up NetFlow correctly by running these commands.

```
#shows the current NetFlow configuration
show ip flow export
#summarizes the active flows and gives an indication of how much NetFlow data the device is
exporting
show ip cache flow or show ip cache verbose flow
```

Sample Flexible Netflow Configuration in IOS

```
flow exporter e1
    ! destination is the collector address, default port needs to be changed to 2055
    destination <accelopsIp>    transport udp 2055
!
flow record r1
    ! record specifies packet fields to collect
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    collect transport tcp flags
    collect interface output
    collect counter bytes
    collect counter packets
!
flow monitor m1
    ! monitor refers record configuration and exporter configuration.
    record r1
    exporter e1
    cache timeout active 60
    cache timeout inactive 30
    cache entries 1000
!
interface GigabitEthernet 2/48
    ip flow monitor m1 input
```

IP SLA

IP SLA is a technology where a pair of routers can run synthetic tests between themselves and report detailed traffic statistics. This enables network administrators to get performance reports between sites without depending on end-host instrumentation.

Cisco provides detailed documents for configuring IP SLA for both general traffic and VoIP.

A variety of IP SLA tests can be run, for example UDP/ICMP Jitter, UDP Jitter for VoIP, UDP/ICMP Echo, TCP Connect, HTTP, etc. You can see the traffic statistics for these these tests by routing appropriate `Show` commands on the router. However, only these IP SLA tests are exported via RTT-MON SNMP MIB.

- UDP Jitter (reported by FortiSIEM event type PH_DEV_MON_IPSLA_MET)
- UDP Jitter for VoIP (reported by FortiSIEM event type PH_DEV_MON_IPSLA_VOIP_MET)
- HTTP performance (reported by FortiSIEM event type PH_DEV_MON_IPSLA_HTTP_MET)
- ICMP Echo (reported by FortiSIEM event type PH_DEV_MON_IPSLA_ICMP_MET)
- UDP Echo (reported by FortiSIEM event type PH_DEV_MON_IPSLA_UDP_MET)

These are the only IP SLA tests monitored by FortiSIEM.

Configuring IP SLA involves choosing and configuring a router to initiate the test and a router to respond. The test statistics are automatically reported by the initiating router via SNMP, so no additional configuration is required. Bi-directional traffic statistics are also reported by the initiating router, so you don't need to set up a reverse test between the original initiating and responding routers. FortiSIEM automatically detects the presence of the IP SLA SNMP MIB (CISCO-RTTMON-MIB) and starts collecting the statistics.

Configuring IP SLA Initiator for UDP Jitter

```
ipsla-init>enable
ipsla-init#config terminal
ipsla-init(config)#ip sla monitor <operation num>ipsla-init(config-sla-monitor)#type jitter
dest-ipaddr <responder ip> dest-port <dest port>ipsla-init(config-sla-monitor-
jitter)#frequency default
ipsla-init(config-sla-monitor-jitter)#exit
ipsla-init(config)# ip sla monitor schedule <operation num> start-time now life forever
```

Configuring IP SLA Initiator for UDP Jitter for VoIP

```
ipsla-init>enable
ipsla-init#config terminal
ipsla-init(config)#ip sla monitor <operation num>ipsla-init(config-sla-monitor)#type jitter
dest-ipaddr <responder ip> dest-port <dest port> codec <codec type> advantage-factor 0
ipsla-init(config-sla-monitor-jitter)#frequency default
ipsla-init(config-sla-monitor-jitter)#exit
```

```
ipsla-init(config)# ip sla monitor schedule <operation num> start-time now life forever
```

Configuring IP SLA Initiator for ICMP Echo Operation

```
Router> enable
Router# configure terminal
Router(config)# ip sla monitor 15
Router(config-sla-monitor)# type echo protocol ipIcmpEcho <destination-ip-address>Router
(config-sla-monitor-echo)# frequency 30
Router(config-sla-monitor-echo)# exit
Router(config)# ip sla monitor schedule 10 start-time now life forever
Router(config)# exit
```

Configuring the IP SLA Responder for All Cases

```
ipsla-resp>enable
ipsla-resp#config terminal
ipsla-resp(config)#ip sla monitor responder
```

Class-Based QoS

CBQoS enables routers to enforce traffic dependent Quality of Service policies on router interfaces for to make sure that important traffic such as VoIP and mission critical applications get their allocated network resources.

Cisco provides detailed documents for configuring IP SLA for both general traffic and VoIP.

The CbQoS statistics are automatically reported by the router via SNMP, so no additional configuration is needs. FortiSIEM detects the presence of valid CBQoS MIBs and starts monitoring them.

NBAR

Cisco provides protocol discovery via NBAR configuration guide.

Make sure that the CISCO-NBAR-PROTOCOL-DISCOVERY-MIB is enabled.

Sample event generated by FortiSIEM

```
[PH_DEV_MON_CISCO_NBAR_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceCisco.cpp,
[lineNumber]=1644,[hostName]=R1.r1.accelops.com,[hostIpAddr]=10.1.20.59,
[intfName]=Ethernet0/0,[appTransportProto]=snmp,[totFlows]=4752,[recvFlows]=3168,
[sentFlows]=1584,[totBytes64]=510127,[recvBytes64]=277614,[sentBytes64]=232513,
[totBitsPerSec]=22528.000000,[recvBitsPerSec]=12288.000000,[sentBitsPerSec]=10240.000000,
[phLogDetail]=
```

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

These are the generic settings for providing SNMP access to your device from FortiSIEM.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has access credentials for your device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password associated with the user

How CPU and Memory Utilization is Collected for Cisco IOS

FortiSIEM follows the process for collecting information about CPU utlization that is recommended by Cisco.

- Monitoring CPU
- Monitoring Memory using PROCESS-MIB

Monitoring CPU

The OID is 1.3.6.1.4.1.9.9.109.1.1.1.1.8. The issue there are multiple CPUs – which ones to take? A sample SNMP walk for this OID looks like this

```
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.1 = Gauge32: 46
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.2 = Gauge32: 22
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.3 = Gauge32: 5
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.8.4 = Gauge32: 4
```

Note that there are 4 CPUs – indexed 1-4. We must identify Control plane CPU and Data plane CPU

The cpu Id -> entity Id mapping from the following SNMP walk

```
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.1 = INTEGER: 3014
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.2 = INTEGER: 3001
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.3 = INTEGER: 1001
SNMPv2-SMI::enterprises.9.9.109.1.1.1.1.2.4 = INTEGER: 7001
```

This provides the following cpu Id -> entity Id mapping

```
1 -> 3014
2 -> 3001
3 -> 1001
4 -> 7001
```

The following SNMP walk provides the names for each entity Id

```
SNMPv2-SMI::mib-2.47.1.1.1.1.7.1001 = STRING: "Chassis 1 CPU of Module 2"SNMPv2-SMI::mib-
2.47.1.1.1.1.7.3001 = STRING: "Chassis 1 CPU of Switching Processor 5"SNMPv2-SMI::mib-
2.47.1.1.1.1.7.3014 = STRING: "Chassis 1 CPU of Routing Processor 5"SNMPv2-SMI::mib-
2.47.1.1.1.1.7.7001 = STRING: "Chassis 2 CPU of Module 2"
```

Combining all this information, we finally obtain the CPU information for each object

```
Chassis 1 CPU of Routing Processor 5 -> 46%
Chassis 1 CPU of Switching Processor 5 -> 22%
Chassis 1 CPU of Module 2 -> 5
Chassis 2 CPU of Module 2 -> 4%
```

FortiSIEM reports utilization per cpu utilization

```
[PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9596,[cpuName]=Chassis 1 CPU of Routing Processor
5,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=46.000000,[pollIntv]=176,
[phLogDetail]=
[PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9596,[cpuName]=Chassis 1 CPU of Switching Processor
5,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=22.000000,[pollIntv]=176,
[phLogDetail]=

PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9596,[cpuName]=Chassis 1 CPU of Module
2,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=5.000000,[pollIntv]=176,
[phLogDetail]=

[PH_DEV_MON_SYS_PER_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9596,[cpuName]=Chassis 2 CPU of Module
2,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,[cpuUtil]=4.000000,[pollIntv]=176,
[phLogDetail]=
```

To get the overall system CPU utilization, we average over “Switching and Routing CPUs”- so CPU Util = (46+22)/2 = 34%

```
PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9611,[cpuName]=RoutingCpu,[hostName]=UB-CORE-SW,[hostIpAddr]=10.11.1.2,
[cpuUtil]=34.0000,[pollIntv]=176,[phLogDetail]=
```

Monitoring Memory using PROCESS-MIB

The relevant OIDs are
Used memory OID = 1.3.6.1.4.1.9.9.48.1.1.1.6
Free memory OID = 1.3.6.1.4.1.9.9.48.1.1.1.5

Memory Util = (Used memory) / (Used memory + Free memory)

```
SNMPv2-SMI::enterprises.9.9.48.1.1.1.5.1 = Gauge32: 87360992  <-  Processor Memory Used
SNMPv2-SMI::enterprises.9.9.48.1.1.1.5.2 = Gauge32: 10715440  <-  IO Memory Used
SNMPv2-SMI::enterprises.9.9.48.1.1.1.6.1 = Gauge32: 2904976  <-  Processor Memory Free
SNMPv2-SMI::enterprises.9.9.48.1.1.1.6.2 = Gauge32: 1342944  <-  IO Memory Free
```

Therefore

```
Used Memory = 98,076,432
Total Memory = 102,324,352
Memory Util = 96%
```

Cisco Meraki Cloud Controller and Network Devices

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Cisco Meraki Devices are discoverable in either of the following ways

- SNMP to the Cloud Controller
- SNMP to each Network Device

SNMP Traps can be sent from the Cloud Controller. Cisco Meraki Network Devices can also send logs directly to FortiSIEM.

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c) to Cloud Controller or Devices	Host name, Software version, Hardware model, Network interfaces	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
syslog from Meraki Firewalls		Firewall logs	Security Monitoring
syslog from Meraki Access Points		Air Marshal logs	Security Monitoring
SNMP Traps from Cloud Controller		Health	Availability Monitoring

Event Types

- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL

Rules

- Availability (From SNMP Trap)
- Performance (Fixed Threshold)

- Performance (Dynamic Threshold Based on Baselines)

Availability (From SNMP Trap)

- Meraki Device Cellular Connection Disconnected
- Meraki Device Down
- Meraki Device IP Conflict
- Meraki Device Interface Down
- Meraki Device Port Cable Error
- Meraki Device VPN Connectivity Down
- Meraki Foreign AP Detected
- Meraki New DHCP Server
- Meraki New Splash User
- Meraki No DHCP lease
- Meraki Rogue DHCP Server
- Meraki Unreachable Device
- Meraki Unreachable RADIUS Server
- Meraki VPN Failover

Performance (Fixed Threshold)

- Network Intf Error Warning
- Network Intf Error Critical
- Network Intf Util Warning
- Network Intf Util Critical

Performance (Dynamic Threshold Based on Baselines)

- Sudden Increase in Network Interface Traffic
- Sudden Increase in Network Interface Errors

Reports

None

Configuration

Syslog for Air Marshal Events

The latest instructions can be found at https://documentation.meraki.com/MR/Monitoring_and_Reporting/Air_Marshal to configure syslog for Air Marshal events.

Syslog alerting can be configured by navigating to **Network-wide > General**, and configuring the syslog server IP, port, and specifying "air marshal" events.

Note: For all roles, select each role available. This configuration applies for access points (APs), switches, and firewalls.

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco Meraki Cloud Controller
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco NX-OS Router and Switch

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	Host name, IOS version, Hardware model, Memory size, Network interface details - name, address, mask and description	Uptime, CPU and Memory utilization, Free processor and I/O memory, Free contiguous processor and I/O memory, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c, V3)	Hardware component details: serial number, model, manufacturer, software and firmware versions of hardware components such as chassis, CPU, fan, power supply, network cards etc.	Hardware health: temperature, fan and power supply	Availability
SNMP (V1, V2c, V3)	Trunk port connectivity between switches and VLANs carried over a trunk port (via CDP MIB), ARP table		Topology and end-host location
SNMP (V1, V2c, V3)	BGP connectivity, neighbors, state, AS number	BGP state change	Routing Topology, Availability Monitoring

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	OSPF connectivity, neighbors, state, OSPF Area	OSPF state change	Routing Topology, Availability Monitoring
SNMP (V1, V2c, V3)		**Class based QoS metrics:** For (router interface, policy, class map) tuple: **class map metrics** including Pre-policy rate, post-police rate, drop rate and drop pct; **police action metrics** including conform rate, exceeded rate and violated rate; **queue metrics** including current queue length, max queue length and discarded packets	QoS performance monitoring
Telnet/SSH	Running and startup configuration, Image file name, Flash memory size, Running processes	Startup configuration change, delta between running and startup configuration, Running process CPU and memory utilization	Performance Monitoring, Security and Compliance
Telnet/SSH	**End host Layer 2 port mapping**: switch interface to VLAN id, end host IP/MAC address association		
Syslog	Device type>	System logs and traffic logs matching acl statements	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco-nxos" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Telnet/SSH

- Syslog
- NetFlow

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device.

- `show startup-config`
- `show running-config`
- `show version`
- `show flash`
- `show context`
- `show ip route`
- `show cam dynamic`
- `show mac-address-table`
- `show mac address-table (for Nexus 1000v)`
- `show vlan brief`
- `show process cpu`
- `show process mem`
- `show disk0`
- `enable`
- `terminal length 0`

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

NetFlow

- Enable NetFlow on the Router
- Create a Flow Template and Define the Fields to Export
- Set up NetFlow Exporter

- Associate the Record to the Exporter Using a Flow Monitor
- Apply the Flow Monitor to Every Interface

Enable NetFlow on the Router

1. Enter configuration mode.
2. Run this command.

   ```
   feature netflow
   ```

Create a Flow Template and Define the Fields to Export

You can can also try using the pre-defined NetFlow template.

```
# show flow record netflow-original
Flow record netflow-original:
    Description: Traditional IPv4 input NetFlow with origin ASs
    No. of users: 1
    Template ID: 261
    Fields:
         match ipv4 source address
         match ipv4 destination address
         match ip protocol
         match ip tos
         match transport source-port
         match transport destination-port
         match interface input
         match interface output
         match flow direction
         collect routing source as
         collect routing destination as
         collect routing next-hop address ipv4
         collect transport tcp flags
         collect counter bytes
         collect counter packets
         collect timestamp sys-uptime first
         collect timestamp sys-uptime last
```

Set up NetFlow Exporter

Run these commands.

```
flow exporter FortiSIEMFlowAnalyzer
description export netflow to FortiSIEM
destination <FortiSIEMIp>export Version 9
transport udp 2055
source vlan613
```

Associate the Record to the Exporter Using a Flow Monitor

In this example the flow monitor is called `FortiSIEMMonitoring`.

Run these commands.

```
flow monitor FortiSIEMMonitoring
exporter FortiSIEMFlowAnalyzer
record netflow-original
```

Apply the Flow Monitor to Every Interface

Run these commands.

```
interface Vlan612
ip flow monitor Monitortac7000 input
exit
interface Vlan613
ip flow monitor Monitortac7000 input
exit
```

You can now check the configuration using the `show` commands.

Settings for Access Credentials

For SNMP, Telnet, and SSH access credentials, see Access Credentials.

Cisco ONS

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial Number, software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP Trap		Alerts	Availability and Performance Monitoring

Event Types

Over 1,800 event types defined. In **ADMIN > Device Support > Event Types**, search for "Cisco-ONS" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco ONS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco Viptela SDWAN Router

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
Syslog	Host name and Device Type from LOG	Over 280 log types	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "viptela" to see the event types associated with this device.

Rules

None

Reports

None

Configuration

Configure Cisco Viptela to send syslog in the supported format to FortiSIEM. No configuration is required in FortiSIEM.

Sample Events

```
<190>430: *Dec  9 05:41:47.025: %Cisco-SDWAN-Router-OMPD-6-INFO-400005: R0/0: OMPD: Number
of vSmarts connected : 2
```

```
CDATA[<187>154: *Aug 23 19:57:51.681: %Cisco-SDWAN-RP_0-OMPD-3-ERRO-400002: R0/0: OMPD:
vSmart peer 1.1.1.5 state changed to Init
```

Dell Force10 Router and Switch

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Dell

Product Information: www.dell.com

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial number, Software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), CPU utilization, Hardware Status	Availability and Performance Monitoring
Syslog			Security and Compliance
Telnet/SSH	Running and Startup configurations	Startup Configuration Change, Difference between Running and Startup configurations	Change monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "force10" to see the event types associated with this device.

The following event types are available:

- Dell-Force10-IFMGR-OSTATE_DN
- Dell-Force10-IFMGR-OSTATE_UP
- Dell-Force10-SEC_LOGIN_SUCCESS
- Dell-Force10-FILEMGR-FILESAVED
- Dell-Force10-SEC_LOGIN_FAILURE
- Dell-Force10-TACACS_ACCESS_ACCEPTED

- Dell-Force10-SSH2-CONF
- Dell-Force10-SYS-CONFIG_I

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Rules**, search for "force10" in the main content panel **Search...** field.

The following reports are available:

- Dell Force10 Interface Extended Performance Metrics
- Dell Force 10 Performance By Component

Configuration

- SNMP
- Syslog
- Telnet/SSH

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

The syslog format should be the same as that shown in the example.

Example Syslog

```
Feb 11 09:50:21: %STKUNIT0-M:CP %IFMGR-5-OSTATE_UP: Changed interface state to up: Te 0/30
190>Jan 6 07:34:34: host1: %STKUNIT0-M:CP %ARPMGR-6-MAC_CHANGE: IP-4-ADDRMOVE: IP address
10.1.48.14 is moved from MAC address 52:54:00:16:5a:74  to MAC address 52:54:00:22:c7:81 .
<189>Jan 4 08:08:43: host1: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user
alchemy on line vty0 ( 10.1.48.201 )
>110>1 2017-01-09T15:41:53.191+08:00 p01-ctl-sw2-d5c2f1 - SEC LOGOUT - INFO: Exec session is
terminated for user meikang on line vty0 ( 192.168.128.202 )
Feb 11 08:36:21 utc: %STKUNIT0-M:CP %IFMGR-5-OSTATE_DN: Changed interface state to down: Te
0/31
```

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device. To initiate discovery and monitoring of your device over this protocol, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

- `show startup-config`
- `show running-config`
- `show version`
- `show ip route`
- `enable`
- `terminal pager 0`

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23

Setting	Value
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Dell N-Series Switch

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Dell

Product Information: www.dell.com

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c)		Hardware Status (Power Supply, Fan)	Availability Monitoring
SSH		Configuration	Change management
Syslog			Security and Compliance

Event Types

- CPU Monitoring: PH_DEV_MON_SYS_CPU_UTIL
- Memory Monitoring: PH_DEV_MON_SYS_MEM_UTIL
- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL
- Hardware Status: PH_DEV_MON_HW_STATUS
- Configuration Change: PH_DEV_MON_CHANGE_STARTUP_CONFIG

- Dell-NSeries-Generic
- Dell-NSeries-Success
- Dell-NSeries-Failed
- Dell-NSeries-Link-Up
- Dell-NSeries-Link-Down
- Dell-NSeries-Logout
- Dell-NSeries-Session-Created
- Dell-NSeries-Temp-Warning
- Dell-NSeries-Temp-Normal
- Dell-NSeries-User-Command
- Dell-NSeries-Invalid-Packet
- Dell-NSeries-SpanningTree-Change
- Dell-NSeries-SpanningTree-Learning-To-Forwarding
- Dell-NSeries-SpanningTree-Learning-To-Blocking
- Dell-NSeries-SpanningTree-Forwarding-To-Blocking
- Dell-NSeries-SpanningTree-Blocking-To-Forwarding

Rules

- Availability
- Performance (Fixed Threshold)
- Performance (Dynamic Threshold Based on Baselines)
- Change

Availability

- Network Device Degraded - Lossy Ping Response
- Network Device Down - no ping response
- Network Device Interface Flapping
- Critical Network Device Interface Staying Down
- Non-critical Network Device Interface Staying Down
- Network Device Hardware Warning
- Network Device Hardware Critical

Performance (Fixed Threshold)

- Network CPU Warning
- Network CPU Critical
- Network Memory Warning
- Network Memory Critical
- Network Intf Error Warning
- Network Intf Error Critical
- Network Intf Util Warning
- Network Intf Util Critical

Performance (Dynamic Threshold Based on Baselines)

- Sudden Increase In System CPU Usage
- Sudden Increase in System Memory Usage
- Sudden Increase in Network Interface Traffic
- Sudden Increase in Network Interface Errors

Change

- Startup Config Change

Reports

- Availability
- Performance
- Change

Availability

- Availability: Router/Switch Ping Monitor Statistics

Performance

- Performance: Top Routers Ranked By CPU Utilization
- Performance: Top Routers By Memory Utilization
- Performance: Top Router Network Intf By Util, Error, Discards
- Top Routers/Switches by Business Hours Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by Business Hours System Uptime Pct (Achieved System SLA)
- Top Routers/Switches by Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by System Uptime Pct (Achieved System SLA)
- Top Router Interfaces by Days-since-last-use

Change

- Change: Router Config Changes Detected Via Login

Configuration

- SNMP
- Syslog

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

The syslog format should be the same as that shown in the example.

Example Syslog

```
<187> Sep 24 13:17:56 Ashley N3048P Switch Stack  1-1 IPV6[dtlTask]: ip6map.c(3787) 89904 %%
Received invalid ip6 packet on Vl1:  TC 0xf3, flow 663552, length 65152, next head 0, hop
lim 0, src 8100:c8::f21f:afff:fedf:2080, dst ff02::1:ffdf:2080.
<187>1 Jan  9 16:03:07.000 192.168.0.15-1 DRIVER[117467844]: broad_hpc_drv.c(4362) 230149630
%% Unit: 0 Blk: 3 MMU MTRO PAR generic parity error.
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell NSeries
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Dell PowerConnect Switch and Router

FortiSIEM Support added: 4.7.2

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Dell

Product Information: www.dell.com

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Serial number, Software version, Hardware model, Network interfaces, Hardware Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), CPU utilization, Hardware Status	Availability and Performance Monitoring
Syslog			Security and Compliance
Telnet/SSH	Running and Startup configurations	Startup Configuration Change, Difference between Running and Startup configurations	Change monitoring

Event Types

There are no event types defined specifically for this device, but event types are prefixed with "Dell-PowerConnect-".

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Syslog
- Telnet/SSH

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

The syslog format should be the same as that shown in the example.

Example Syslog

```
<189> Apr 13 15:21:08 192.168.5.43-1 CLI_WEB[103917236]: cmd_logger_api.c(140) 5203 %%
WEB:192.168.5.101:admin:User requested /VLAN_Membership.html url
<189> Apr 13 15:21:18 192.168.5.43-1 CLI_WEB[103917236]: cmd_logger_api.c(140) 5204 %%
WEB:192.168.5.101:admin:User admin logged out
<190> Apr 13 15:19:32 192.168.5.43-1 CLI_WEB[103917236]: cmd_logger_api.c(260) 5199 %%
[CLI:admin:192.168.5.15] User has succesfully logged in
<189> Jun 30 16:04:24 Switch-2-1 TRAPMGR[trapTask]: traputil.c(735) 47619 %% 'startup-
config' has changed.
<190> Jun 30 16:04:24 Switch-2-1 UNITMGR[emWeb]: unitmgr.c(6778) 47618 %% Configuration
propagation successful for config type 0
```

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

These commands are used for discovery and performance monitoring via SSH. Please make sure that the access credentials you provide in FortiSIEM have the permissions necessary to execute these commands on the device. To initiate discovery and monitoring of your device over this protocol. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

- `show startup-config`
- `show running-config`
- `show version`
- `show ip route`
- `enable`
- `terminal pager 0`

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell PowerConnect
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Foundry Networks IronWare Router and Switch

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, Ironware version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
Telnet/SSH	Running and startup configuration	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
SNMP (V1, V2c)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location
Syslog	Device type	System logs and traffic logs matching acl statements	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "foundry-ironware" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Telnet/SSH
- Syslog
- Sample Parsed PowerConnect Syslog Message

SNMP

1. Log in to the device manager for your switch or router with administrative privileges.
2. Enter configuration mode.
3. Run these commands to set the community string and enable the SNMP service.

```
snmp-server community <community> RO
snmp-server enable vlan <vlan id>
```

4. Exit config mode.
5. Save the configuration.

Telnet/SSH

FortiSIEM uses Telnet/SSH to communicate with this device. Refer to the product documentation for your device to enable Telnet/SSH.

Syslog

1. Log in to the device manager for your switch or router with administrative privileges.
2. Enter configuration mode.
3. Run this command to set your FortiSIEM virtual appliance as the recipient of syslog from your router or switch.

```
logging host <FortiSIEM Ip>
```

4. Exit config mode.
5. Save the configuration.

Sample Parsed PowerConnect Syslog Message

```
<14>SJ-Dev-A-Fdy-FastIron, running-config was changed from console

<14>SJ-Dev-A11-Fdy-FastIron, startup-config was changed from telnet client 192.168.20.18
<14>SJ-Dev-A-Fdy-FastIron, phoenix_agent login to USER EXEC mode

<14>SJ-Dev-A-Fdy-FastIron, Interface ethernet3, state up

<14>SJ-Dev-A-Fdy-FastIron, Interface ethernet 20/3, state up

<12>SJ-QA-A-Fdy-BigIron, list 100 permitted udp 173.9.142.98(ntp)(Ethernet 2/1
0004.23ce.ba11) -> 172.16.20.121(ntp), 1 event(s)

<14>SJ-Dev-A-Fdy-FastIron, Bridge root changed, vlan 3, new root ID 80000004806137c6, root
interface 3

<14>SJ-QA-A-Fdy-BigIron, VLAN 4 Port 2/7 STP State -> DISABLED (PortDown)

Jun  4 15:51:18 172.16.20.99 Security: telnet logout by admin from src IP 137.146.28.75, src
MAC 000c.dbff.6d00

Jun  4 15:51:12 172.16.20.100 System: Interface ethernet 4/9, state down

Jun  4 03:12:53 172.16.20.100 ACL: ACL: List GWI-in permitted tcp 61.158.162.230(6000)
(Ethernet 1/4 0023.3368.f500) -> 137.146.0.0(8082), 1 event(s)

Jun  4 02:54:31 172.16.20.100 ACL: ACL: List XCORE denied udp 137.146.28.75(55603)(Ethernet
1/1 000c.dbde.6000) -> 137.146.3.35(snmp), 1 event(s)

Jun  4 01:49:09 172.16.20.100 STP: VLAN 3104 Port 4/22 STP State -> LEARNING (FwdDlyExpiry)
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

- Foundry Ironware
- SNMP Access Credentials for All Devices
- Telnet Access Credentials for All Devices
- SSH Access Credentials for All Devices

Foundry Ironware

Setting	Value
Name	<set name>
Device Type	Foundry Ironware

Setting	Value
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Telnet Access Credentials for All Devices

These are the generic settings for providing Telnet access to your device from FortiSIEM.

Setting	Value
Name	Telnet-generic
Device Type	generic
Access Protocol	Telnet
Port	23
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22

Setting	Value
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

HP/3Com ComWare Switch

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware status: Power Supply, Fan, Temperature	Availability and Performance Monitoring
SNMP (V1, V2c, V3)		Hardware status: Temperature	Availability
Syslog		System logs	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "comware" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Syslog

- Example Syslog for ComWare Switch Messages

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Example Syslog for ComWare Switch Messages

```
%Apr 2 11:38:11:113 2010 H3C DEVD/3/BOARD REBOOT:Chasis 0 slot 2 need be rebooted
automatically!
%Sep 22 20:38:32:947 2009 H3C DEVD/4/BRD MISPLUG: The board or subcard in slot 1 is not
supported.
%Sep 22 20:38:32:947 2009 H3C DEVD/4/BRD MISPLUG: The board type of MR in 1 is different
from the Mate MR's, so the MR can't work properly.
%Sep 22 20:38:32:947 2009 H3C DEVD/2/BRD TOO HOT:Temperature of the board is too high!
%Sep 22 20:38:32:947 2009 H3C DEVD/2/ FAN CHANGE: Chassis 1: Fan communication state
changed: Fan 1 changed to fault.
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	H3C Comware
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

HP ProCurve Switch

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware status: Power Supply, Fan, Temperature	Availability and Performance Monitoring
Telnet/SSH	Running and startup configuration	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
SNMP (V1, V2c)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location

Event Types

In **ADMIN > Device Support > Event Types**, search for "procurve" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Telnet/SSH

SNMP

1. Go to **Configuration > SNMP Community > V1/V2 Community**.
2. Enter a **Community Name**.
3. For **MIB-View**, select **Operator**.
4. For Write-Access, leave the selection cleared.
5. Click **Add**.

Telnet/SSH

1. Log into the device manager for your ProCurve switch.
2. Go to **Security > Device Passwords**.
3. Create a user and password for **Read-Write Access**.
   Although FortiSIEM does not modify any configurations for your switch, Read-Write Access is needed to read the device configuration.
4. Go to **Security > Authorized Addresses** and add the FortiSIEM IP to Telnet/SSH.
   This is an optional step.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	HP ProCurve
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

HP Value Series (19xx) and HP 3Com (29xx) Switch

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SSH		Configuration	Change management

Event Types

- CPU Monitoring: PH_DEV_MON_SYS_CPU_UTIL
- Memory Monitoring: PH_DEV_MON_SYS_MEM_UTIL
- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL
- Configuration Change: PH_DEV_MON_CHANGE_STARTUP_CONFIG

Rules

- Availability
- Performance (Fixed Threshold)
- Performance (Dynamic Threshold Based on Baselines)
- Change

Availability

- Network Device Degraded - Lossy Ping Response
- Network Device Down - no ping response
- Network Device Interface Flapping
- Critical Network Device Interface Staying Down
- Non-critical Network Device Interface Staying Down

Performance (Fixed Threshold)

- Network CPU Warning
- Network CPU Critical
- Network Memory Warning
- Network Memory Critical
- Network Intf Error Warning
- Network Intf Error Critical
- Network Intf Util Warning
- Network Intf Util Critical

Performance (Dynamic Threshold Based on Baselines)

- Sudden Increase In System CPU Usage
- Sudden Increase in System Memory Usage
- Sudden Increase in Network Interface Traffic
- Sudden Increase in Network Interface Errors

Change

- Startup Config Change

Reports

- Availability
- Performance
- Change

Availability

- Availability: Router/Switch Ping Monitor Statistics

Performance

- Performance: Top Routers Ranked By CPU Utilization
- Performance: Top Routers By Memory Utilization
- Performance: Top Router Network Intf By Util, Error, Discards
- Top Routers/Switches by Business Hours Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by Business Hours System Uptime Pct (Achieved System SLA)
- Top Routers/Switches by Network Ping Uptime Pct (Achieved Network Ping SLA)
- Top Routers/Switches by System Uptime Pct (Achieved System SLA)
- Top Router Interfaces by Days-since-last-use

Change

- Change: Router Config Changes Detected Via Login

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	HP VSeries
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Hirschmann SCADA Firewalls and Switches

What is Discovered and Monitored

Protocol	Information Discovered	Metrics/LOG collected	Used for
SNMP	Host Name	SNMP – Uptime, CPU, Memory, Interface utilization, hardware Status, OSPF metrics	Performance Monitoring

Event Types

The following event types are used for performance monitoring:

- `PH_DEV_MON_SYS_UPTIME` - Uptime monitoring
- `PH_DEV_MON_SYS_CPU_UTIL` – CPU utilization
- `PH_DEV_MON_SYS_MEM_UTIL` – Memory utilization
- `PH_DEV_MON_NET_INTF_UTIL` – Interface utilization
- `PH_DEV_MON_HW_STATUS` – Hardware status

Rules

All performance monitoring rules apply.

Reports

All performance monitoring reports apply.

Configuration

Configure Hirschmann firewalls and switches for SNMP V1/V2c/V3 discovery and performance monitoring. Define the basic SNMP credentials on FortiSIEM and discover these devices. See SNMP Access Credentials.

Sample Events

The events are standard for all devices.

Juniper Networks JunOS Switch

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, JunOS version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Hardware status: Power Supply, Fan, Temperature	Availability and Performance Monitoring
Telnet/SSH	Running and startup configuration	Startup configuration change, delta between running and startup configuration	Performance Monitoring, Security and Compliance
SNMP (V1, V2c, V3)	Trunk port connectivity between switches and VLANs carried over a trunk port, End host Layer 2 port mapping: switch interface to VLAN id, end host IP/MAC address association		Topology and end-host location
Syslog		System logs and traffic logs matching acl statements	Availability, Security and Compliance
sflow		Traffic flow	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "junos" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Syslog
- Sample JunOS Syslog Messages
- sFlow

SNMP

1. Log in to the device manager for your JunOS switch with administrator privileges.
2. Go to **Configure > Services > SNMP**.
3. Under **Communities**, click **Add**.
4. Enter a **Community Name**.
5. Set **Authorization** to **read-only**.
6. Click **OK**.

Syslog

1. Log in to the device manager for your JunOS switch with administrator privileges.
2. Go to **Dashboard > CLI Tools > CLI Editor**.

   Edit the `syslog` section to send syslog to FortiSIEM.
3. **JunOS Syslog Configuration**

```
system {
   ....
   syslog {
       user * {
            any emergency;
       }
       host <FortiSIEM Ip> {
            any any;
            explicit-priority;
       }
       file messages {
            any notice;
            authorization info;
       }
       file interactive-commands {
            interactive-commands any;
       }
       time-format year millisecond;
   }
....
}
```

4. Click **Commit**.

Sample JunOS Syslog Messages

```
190>May 11 13:54:10 20.20.20.20 mgd[5518]: UI_LOGIN_EVENT: User 'phoenix_agent' login, class
'j-super-user' [5518], ssh-connection '192.168.28.21 39109 172.16.5.64 22', client-mode
'cli'

<38>Nov 18 17:50:46 login: %AUTH-6-LOGIN_INFORMATION: User phoenix_agent logged in from host
192.168.20.116 on device ttyp0
```

sFlow

Routing the sFlow Datagram in EX Series Switches

According to Juniper documentation, the sFlow datagram **cannot** be routed over the management Ethernet interface (`me0`) or virtual management interface (`vme0`) i n an EX Series switch implementation. It can only be exported over the network Gigabit Ethernet or 10-Gigabit Ethernet ports using valid route information in the routing table.

1. Log in to the device manager for your JunOS switch with administrator privileges.
2. Go to **Configure > CLI Tools > Point and Click CLI**.
3. Expand **Protocols** and select **slow**.
4. Next to **Collector**, click **Add new entry**.
5. Enter the **IP** address for your FortiSIEM virtual appliance.
6. For **UDP Port**, enter **6343**.
7. Click **Commit**.
8. Next to **Interfaces**, click **Add new entry**.
9. Enter the **Interface Name** for all interfaces that will send traffic over sFlow.
10. Click **Commit**.
11. To disable the management port, go to **Configure > Management Access**, and remove the address of the management port.
    You can also disconnect the cable.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>

Setting	Value
Device Type	Juniper JunOS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

MikroTik Router

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	MikroTik RouterOS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Nortel ERS and Passport Switch

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c)	Host name, software version, Hardware model, Network interfaces,	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP (V1, V2c)		Hardware status: Temperature	
SNMP (V1, V2c, V3)		Layer 2 port mapping: associating switch ports to directly connected host IP/MAC addresses	Identity and location table; Topology

Event Types

There are no event types defined specifically for this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Nortel ERS / Nortel Passport
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Security Gateways

FortiSIEM supports these security gateways for discovery and monitoring.

- Barracuda Networks Spam Firewall
- Blue Coat Web Proxy
- Cisco IronPort Mail Gateway
- Cisco IronPort Web Gateway
- Fortinet FortiMail
- Fortinet FortiProxy
- Fortinet FortiWeb
- Imperva SecureSphere DB Monitoring Gateway
- Imperva SecureSphere DB Security Gateway
- McAfee Vormetric Data Security Manager
- McAfee Web Gateway
- Microsoft ISA Server
- Oracle Cloud Access Security Broker (CASB)
- Proofpoint
- Squid Web Proxy
- SSH Comm Security CryptoAuditor
- Websense Web Filter

Barracuda Networks Spam Firewall

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, Interfaces, Serial number	CPU utilization, Memory utilization, Interface Utilization	Performance Monitoring
Syslog		Various syslog - scenarios include - mail scanned and allowed/denied/quarantined etc; mail sent and reject/delivered/defer/expired; mail received and allow/abort/block/quarantined etc.	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "barracuda" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Syslog
- Sample Parsed Barracuda Spam Firewall Syslog Message

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.
- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Sample Parsed Barracuda Spam Firewall Syslog Message

```
<23>inbound/pass1[923]: 127.0.0.1 1300386119-473aa6a90001-sB89EM 0 0 RECV - 1 4D760309475
250 2.6.0  <E6BB7C56C6761D42AEAFBF7FC6E17E920156A38D@USNSSEXC174.us.kworld.kpmg.com> Queued
mail for delivery

<23>scan[9390]: mail.netcontentinc.net[207.65.119.227] 1300386126-4739a8be0001-R6OEVB
1300386126 1300386128 SCAN - release@calcium.netcontentinc.net kmcgilvrey@qinprop.com - 7 61
- SZ:34602 SUBJ:How FMLA Leave, ADA and Workers' Compensation Work Together April 28, 2011
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Barracuda Spam Firewall
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Blue Coat Web Proxy

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, Interfaces, Serial number	CPU utilization, Memory utilization	Performance Monitoring
SNMP		**Proxy performance**: Proxy cache object count, Proxy-to-server metrics: HTTP errors, HTTP requests, HTTP traffic (KBps); Server-to-proxy metrics: HTTP traffic (KBps), Client-to-proxy metrics: HTTP requests, HTTP Cache hit, HTTP errors, HTTP traffic (KBps); Proxy-to-client metrics: HTTP traffic (KBytes)	Performance Monitoring
SFTP		**Proxy traffic**: attributes include Source IP, Destination IP, Destination Name, Destination Port, URL, Web category, Proxy action, HTTP User Agent, HTTP Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance
Syslog		Admin authentication success and failure	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "blue coat" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Syslog
- Sample Parsed Blue Coat Audit Syslog
- SFTP

SNMP

The following procedures enable FortiSIEM to discover Bluecoat web proxy.

1. Log in to your Blue Coat management console.
2. Go to **Maintenance > SNMP**.
3. Under **SNMP General**, select **Enable SNMP**.
4. Under Community Strings, click Change Read Community, and then enter a community string that FortiSIEM can use to access your device.
5. Click **OK**.

Syslog

Syslog is used by Blue Coat to send audit logs to FortiSIEM.

1. Log in to your Blue Coat management console.
2. Go to **Maintenance > Event Logging**.
3. Under **Level**, select **Severe Errors**, **Configuration Events**, **Policy Messages**, and **Informational**.
4. Under **Syslog**, enter the IP address of your FortiSIEM virtual appliance for **Loghost**.
5. Select **Enable syslog**.
6. Click **Apply**.

Sample Parsed Blue Coat Audit Syslog

```
<2> Sep 14 19:24:39 ao BluecoatAuthWebLog   0       2010-09-14 14:31:13 36 34.159.60.56
hz13321 - - OBSERVED "Audio/Video Clips" - 200 TCP_NC_MISS POST application/x-fcs http
213.200.94.86 80 /idle/WdPmdz02xSLO2sHS/25136 - - "Shockwave Flash" 34.160.179.201 1087 217
-
```

SFTP

SFTP is used to send access logs to FortiSIEM. Access logs includes the traffic that Blue Coat proxies between the client and the server. The access logs are sent via FTP, where Bluecoat is the client and FortiSIEM is the server. You must configure SFTP in FortiSIEM first, and then on your Blue Coat web proxy server.

Configure FTP in FortiSIEM

1. Log in to your Supervisor node as `root`.
2. Change directory to `/opt/phoenix/bin`.
3. Run the `./phCreateBluecoatDestDir` command to create an FTP user account.
   The files sent from Blue Coat will be temporarily stored in this account. The script will create an user called `ftpuser`. If the this user already exists, you do not need to create a new one. The script will ask for the IP address of Blue Coat and the password for the user `ftpuser`, and will then create the directory `/opt/phoenix/cache/bluecoat/<Bluecoat IP>`.
4. Run `vi /etc/passwd` to change the home directory for `ftpuser` to `/opt/phoenix/cache/bluecoat`. Change only the home directory, do not change any other value.

Configure an Epilog Client in FortiSIEM

The Epilog client converts each line of the log files in the `/opt/phoenix/cache/bluecoat/<Bluecoat IP>` directory in real time into a syslog, and sends it to the FortiSIEM parser for processing.

1. Log in to your Supervisor or the Collector node as `root`.
2. Update the Epilog configuration in `/etc/snare/epilog/epilog.conf` as shown in this code block, and then restart the epilog daemon with the `/etc/init.d/epilogd restart` command.

```
Output
network=localhost:514
syslog=2
Input
log=BluecoatWebLog:/opt/phoenix/cache/bluecoat/172.16.0.141/SG_FortiSIEM_bluecoat_
main.log
log=BluecoatImLog:/opt/phoenix/cache/bluecoat/172.16.0.141/SG_FortiSIEM_bluecoat_im.log
log=BluecoatImLog:/opt/phoenix/cache/bluecoat/172.16.0.141/SG_FortiSIEM_bluecoat_ssl.log
log=BluecoatP2pLog:/opt/phoenix/cache/bluecoat/172.16.0.141/SG_FortiSIEM_bluecoat_
p2p.log
```

Configure FTP in Blue Coat

1. Log in to your Blue Coat management console.
2. Go to **Management Console > Configuration > Access Logging > General**.
3. Select **Enable Access Logging**.
4. In the left-hand navigation, select **Logs**.
5. Under **Upload Client**, configure these settings.

Setting	Value
Log	main
Client Type	FTP Client
Encryption Certificate	No Encryption

Setting	Value
Keyring Signing	No Signing
Save the log file as	text file
Send partial buffer after	1 seconds
Bandwidth Class	<none>

6. Next to **Client Type**, click **Settings**.
7. Configure these settings.

Setting	Value
Settings for	Primary FTP Server
Host	IP address of your FortiSIEM virtual appliance
Port	514
Path	/<Blue Coat IP Address>
Username	ftpuser
Change Primary Password	Use the password you created for `ftpuser` in FortiSIEM
Filename	`SG_FortiSIEM_bluecoat_main.log`

8. Clear the selections **Use Secure Connections (SSL)** and **Use Local Time**.
9. Select **Use Pasv**.
10. Click **OK**.
11. Follow this same process to configure the settings for im, ssl and p2p. For each of these, you will refer to a different **Filename**.
    - For im the file name is `SG_FortiSIEM_bluecoat_im.log`
    - For ssl the file name is `SG_FortiSIEM_bluecoat_ssl.log`
    - For p2p the file name is `SG_FortiSIEM_bluecoat_p2p.log`

Sample Parsed Blue Coat Access Syslog

```
<2> Jun 25 11:15:33 SJ-QA-W-FDR-Test-01.prospect-hills.net BluecoatWebLog       0       2010-06-25
18:13:34 2021 192.168.22.21 200 TCP_TUNNELED 820 1075 CONNECT tcp accelops.webex.com 443 / -
- - NONE 172.16.0.141 - - "WebEx Outlook Integration Http Agent" PROXIED "none" -
25.24.23.22
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Blue Coat CacheOS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco IronPort Mail Gateway

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP		Ping Status, SNMP Ping Stat, Uptime, CPU Util, Mem Util, Net Intf Stat, Hardware Status	
Syslog		**Mail attributes**: attributes include MID, ICID, DCID, Sender address, Receiver Address, Mail Subject, Sent Bytes, Attachment, Spam indicator, Virus indicator, Quarantine indicator, SMTP delivery failures and failure codes, mail action - pass, block, clean.	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "ironport-mail" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "ironport mail" in the main content panel **Search...** field to see the reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

1. Log in to your Ironport Mail Gateway device manager with administrator privileges.
2. Edit the Log Subscription settings.
3. For **Log Name**, enter **IronPort-Mail**.
   This identifies the log to FortiSIEM as originating from an Ironport mail gateway device.
4. For **Retrieval Method**, select **Syslog Push**.
5. For **Hostname**, enter the IP address of your FortiSIEM virtual appliance.
6. For **Protocol**, select **UDP**.

Sample Parsed Ironport Mail Gateway Syslog

```
Tue Sep 24 11:39:49 2012 IronPort-Mail: Info: MID 200257071 ready 24663 bytes from
<someone@foo.com>Sep 24 11:39:49 18.0.19.8 IronPort-Mail: Info: MID 1347076 ICID 346818
From: <john.doe@abc.com>Tue Sep 24 11:39:49 2012 IronPort-Mail: Info: Message aborted MID
200257071 Dropped by antivirus
Tue Sep 24 11:39:49 2012 IronPort-Mail: Info: Delayed: DCID 5 MID 200257071 to RID 0 - 4.1.0
- Unknown address error ('466', ['Mailbox temporarily full.'])[]
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco IronPort AsyncOS Mail
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco IronPort Web Gateway

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		**Squid style web logs**: attributes include Source IP Address, Destination Host name, Sent Bytes, Received Bytes, HTTP User Agent, HTTP Referrer, HTTP Version, HTTP Method, HTTP Status Code, URL, HTTP Content type, Web Category, HTTP Proxy Action	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "ironport-web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- Syslog
- Sample Parsed Ironport Web Gateway Syslog

Syslog

1. Log in to your Ironport gateway device manager with administrator privileges.
2. Edit the settings for Log Subscription.

Setting	Value
Log Type	Access Logs
Log Name	IronPort-Web This identifies the log to FortiSIEM as originating from an IronPort web gateway device
Log Style	Squid
Custom Fields	`%L %B %u`
Enable Log Compression	Clear the selection
Retrieval Method	Syslog Push
Hostname	The IP address of your FortiSIEM virtual appliance
Protocol	UDP

Sample Parsed Ironport Web Gateway Syslog

```
<134>Oct 09 09:19:25 IronPort-Web: Info: 1349795965.314 92 10.163.154.153 TCP_CLIENT_
REFRESH_MISS/200 70798 GET
http://forefrontdl.microsoft.com/server/scanengineupdate/x86/Kaspersky/Package/1210090007/ba
ses/base1b1d.kdc.cab - DIRECT/forefrontdl.microsoft.com application/octet-stream ALLOW_
CUSTOMCAT_11-UnAuthenticated_Applications-APU_No_Auth-NONE-NONE-NONE-DefaultGroup <J_
Doe,6.9,-,""-"",-,-,-,-,""-"",-,-,-,""-"",-,-,""-"",""-"",-,-,IW_swup,-,""-"",""-
"",""Unknown"",""Unknown"",""-"",""-"",6156.35,0,-,""-"",""-""> - ""09/Oct/2012:09:19:25 -
0600"" 71052 ""V3S;{6ADC64A3-11F9-4B04-8257-BEB541BE2975};""
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco IronPort AsyncOS Web
Access Protocol	See Access Credentials
Port	See Access Credentials

Setting	Value
Password config	See Password Configuration

Fortinet FortiMail

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		System events (e.g. configuration changes), System up/down/restart events, Performance issues, Admin logon events, malware attachments	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortimail" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortimail" in the main content panel **Search...** field to see the rules associated with this device.

For generic availability rules, see **RESOURCES > Rules > Availability > Network**.

For generic performance rules, see **RESOURCES > Rules > Performance > Network**.

Reports

In **RESOURCES > Reports**, search for "fortimail" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- Syslog
- Sample Parsed FortiMail Syslog

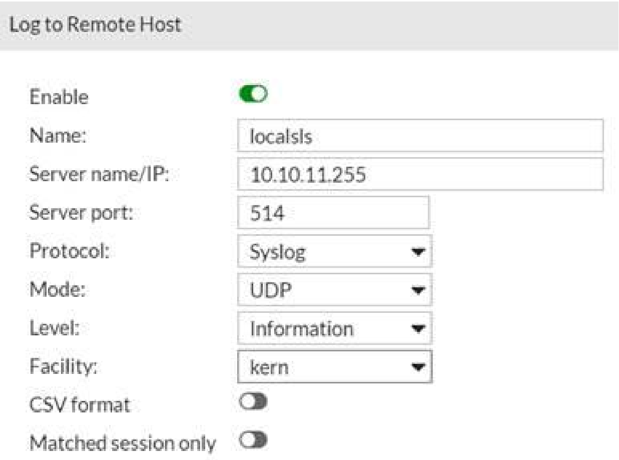
Syslog

Configure FortiMail appliance to send logs to FortiSIEM. Make sure the format matches.

In the FortiMail GUI go to **Log & Report > Log Setings > Remote (tab) > New**.

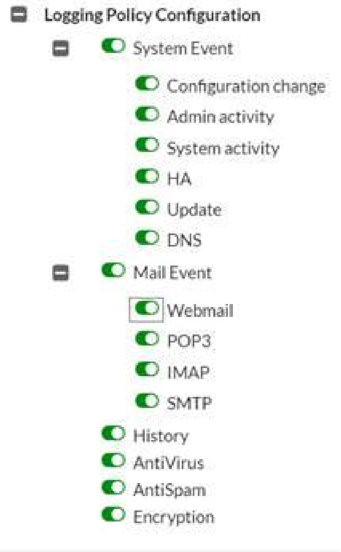
Suggested Logging configuration:

Name	Description
Name	Define a name for the configuration.
Server name/IP	Enter the resolvable DNS name or IP of the FortiSIEM appliance where logs will be sent.
Server port	514
Mode	UDP
Level	Information
Facility	kern
CSV format	leave disabled
Matched session only	leave disabled



Log to Remote Host

Enable	●
Name:	localsls
Server name/IP:	10.10.11.255
Server port:	514
Protocol:	Syslog
Mode:	UDP
Level:	Information
Facility:	kern
CSV format	○
Matched session only	○



Sample Parsed FortiMail Syslog

```
date=2012-08-17 time=12:26:41 device_id=FE100C3909600504 log_id=0001001623 type=event
subtype=admin pri=information user=admin ui=GUI(172.20.120.26) action=login status=success
reason=none msg="User admin login successfully from GUI(172.20.120.26)"
date=2012-07-16 time=12:22:56 device_id=FE100C3909600504 log_id=0200001075 type=statistics
pri=information session_id="q6GJMuPu003642-q6GJMuPv003642" client_name="[172.20.140.94]"
dst_ip="172.20.140.92" endpoint="" from="user@external.lab" to="user5@external.lab"
subject=""mailer="mta" resolved="OK" direction="in" virus="" disposition="Reject"
classifier="Recipient Verification" message_length="188"
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiMail
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Fortinet FortiProxy

FortiSIEM Support added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Fortinet

Product Information: https://www.fortinet.com/products/secure-web-gateway/fortiproxy

- Log Information
- Event Types
- Rules
- Reports

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortiproxy" to see the event types associated with this device.

In 6.3.1, there are over 14,000 event types.

Rules

In **RESOURCES > Rules**, search for "fortiproxy" in the main content panel **Search...** field to see related rules associated with this device.

- FortiAI: Attack Chain Blocked
- FortiAI: Attack Chain Permitted

Reports

In **RESOURCES > Reports**, search for "fortproxy" in the main content panel **Search...** field to see the reports associated with this device.

In FortiSIEM 6.3.1, there are 12 reports available.

- FortiProxy Admin Authentication Events
- FortiProxy App Control App Group Name Summary
- FortiProxy App Control App Name Summary
- FortiProxy App Control Detailed
- FortiProxy UTM Event Summary
- FortiProxy WebFilter Blocked and Passthrough Event Count
- FortiProxy WebFilter Blocked Event Count
- FortiProxy Web Filter Detailed

- FortiProxy Web Filter Events by Web Category, User, and Count
- FortiProxy Webfilter Group by Action,Category, and Count
- FortiProxy WebFilter Passthrough Event Count
- FortiProxy Web Filter User Hit Count

Fortinet FortiWeb

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP	Host Name, Vendor, Model, Version, Hardware Model, hardware	CPU, memory, Disk, Interface, Uptime	Performance monitoring
Syslog		System events (e.g. configuration changes), System up/down/restart events, Performance issues, Admin logon events, Security exploits	Security Monitoring and compliance

Supported Syslog format

Currently FortiSIEM supports FortiWeb native logging format and not CEF format.

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortiweb" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortiweb" in the main content panel **Search...** field to see the rules associated with this device.

For generic availability rules, see **RESOURCES > Rules > Availability > Network**.

For generic performance rules, see **RESOURCES > Rules > Performance > Network**.

Reports

In **RESOURCES > Reports**, search for "fortiweb" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- Syslog
- Sample FortiWeb Syslog

Syslog

Configure FortiWeb appliance to send logs to FortiSIEM. Make sure the format matches. Configuration steps can be found in the FortiWeb Administration Guide Logging section. Remember to point your syslog policy to the FortiSIEM collector IP address.

Sample FortiWeb Syslog

```
date=2016-02-18 time=10:00:05 log_id=00001002 msg_id=000067508821 device_
id=FV400D3A15000010 vd="root" timezone="(GMT+3:00)Baghdad" type=event subtype="admin"
pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User
admin changed global from GUI(172.22.6.66)
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiWeb
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Imperva SecureSphere DB Monitoring Gateway

- Configuration in FortiSIEM

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	<set name>
Device Type	Imperva Securesphere DB Monitoring Gateway
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration
User Name	A user who has access credentials for the device
Password	The password for the user
Super Password	Password for Super

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Imperva SecureSphere DB Monitoring Gateway.
5. To see the jobs associated with Imperva, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Imperva" in the search box.

Imperva SecureSphere DB Security Gateway

- What is Discovered and Monitored
- Configuration
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)			Security and Compliance

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	<set name>
Device Type	Imperva Securesphere DB Security Gateway
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration
User Name	A user who has access credentials for the device
Password	The password for the user
Super Password	Password for Super

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list, and select **Test Connectivity** to test the connection to Imperva SecureSphere DB Security Gateway.

5. To see the jobs associated with Imperva, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Imperva" in the search box.

Sample Events

```
<14>CEF:0|Imperva Inc.|SecureSphere|11.5.0.20_0|Audit|Audit|Informative|dst=10.2.6.194
dpt=3306 duser=wf_settlement src=10.2.6.48 spt=59876 proto=TCP rt=11 April 2016 14:07:09
cat=Audit Default Rule - All cs2Label=ServerGroup cs3=ProcessMakerDBFX cs3Label=ServiceName
cs4=Default MySql Application cs4Label=ApplicationName cs5=642697783064 cs5Label=EventId
cs6=Query cs6Label=EventType cs7=Default MySql group cs7Label=UserGroup cs8=True
cs8Label=UserAuthenticated cs9= cs9Label=ApplicationUser cs10= cs10Label=SourceApplication
cs11= cs11Label=OSUser cs12= cs12Label=HostName cs13=wf_settlement cs13Label=Database cs14=
cs14Label=Schema cs15=SELECT COUNT(APP_CACHE_VIEW.APP_UID) FROM APP_CACHE_VIEW LEFT JOIN
USERS CU ON (APP_CACHE_VIEW.USR_UID=CU.USR_UID) LEFT JOIN USERS PU ON (APP_CACHE_
VIEW.PREVIOUS_USR_UID=PU.USR_UID) LEFT JOIN APP_CACHE_VIEW APPCVCR ON (APP_CACHE_VIEW.APP_
UID=APPCVCR.APP_UID AND APPCVCR.DEL_LAST_INDEX=1) LEFT JOIN USERS USRCR ON (APPCVCR.USR_
UID=USRCR.USR_UID) WHERE APP_CACHE_VIEW.APP_STATUS='TO_DO' AND APP_CACHE_VIEW.USR_
UID='2800810224bbdfe1cc8bb02024369548' AND APP_CACHE_VIEW.DEL_FINISH_DATE IS NULL  AND APP_
CACHE_VIEW.APP_THREAD_STATUS='OPEN' AND APP_CACHE_VIEW.DEL_THREAD_STATUS='OPEN'
cs15Label=RawQuery cs16=select count(app_cache_view.app_uid) from app_cache_view left join
users cu on (app_cache_view.usr_uid=cu.usr_uid) left join users pu on (app_cache_
view.previous_usr_uid=pu.usr_uid) left join app_cache_view appcvcr on (app_cache_view.app_
uid=appcvcr.app_uid and appcvcr.del_last_index=?) left join users usrcr on (appcvcr.usr_
uid=usrcr.usr_uid) where app_cache_view.app_status=? and app_cache_view.usr_uid=? and app_
cache_view.del_finish_date is ? and app_cache_view.app_thread_status=? and app_cache_
view.del_thread_status=? cs16Label=ParsedQuery cs17= cs17Label=BindVariables cs18=
cs18Label=SQLError cs19=1 cs19Label=ResponseSize cs20=0 cs20Label=ResponseTime cs21=0
cs21Label=AffectedRows
```

McAfee Vormetric Data Security Manager

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)		1 event type	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "Vormetric-" in the main content panel **Search...** field.

Sample Event Type

```
<14> 2013-06-29T18:44:42.420Z 10.10.10.1 CEF:0|Vormetric, Inc.|dsm|5.2.0.1|DAO0048I|update
host|3|cs4Label=logger cs4=DAO spid=4322 rt=1388986263954 dvchost=example.com suser=USER_1
shost=test_cpu
```

Rules

There are no specific rules but generic rules for Security Manager and Generic Servers apply.

Reports

There are no specific reports but generic rules for Security Manager and Generic Servers apply.

Configuration

Configure Vormetric Data Security Manager to send syslog in CEF format on port 514 to FortiSIEM.

McAfee Web Gateway

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		**Parsed event attributes**: include Source IP, Destination URL, HTTP Method, HTTP User agent, HTTP Status Code, HTTP Content Type, Blocked Reason, Risk	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "mcafee-web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- Syslog
- Sample Parsed McAffee Web Gateway Syslog Message

Syslog

FortiSIEM processes events from this device via syslog sent by the device. Configure the device to send syslog to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server**, or the server where the syslog should be sent, enter the IP address of your FortiSIEM virtual appliance.
- For **Port**, enter **514**.

- Make sure that the syslog type is **Common Event Format** (CEF). The syslog format should be the same as that shown in the example.

Sample Parsed McAffee Web Gateway Syslog Message

```
[21/Feb/2012:11:44:19  -0500]  """"""""""""    ""10.200.11.170 200 """"GET http://abc.com/
HTTP/1.1"""" """"General News"""" """"Minimal Risk"""" """"text/html"""" 101527 """"""""
"""""""" """"0""""""[30/May/2012:10:39:44 -0400] "" 10.19.2.63 200
"GEThttp://abc.com/html.ng/site=cnn&cnn_pagetype=main&cnn_position=126x31_spon2&cnn_
rollup=homepage&page.allowcompete=no&params.styles=fs&Params.User.UserID=4fc6251c068c9f0aa51
475025d0040b8&transactionID=7179860628805012&tile=4893878838331&domId=135492 HTTP/1.1" "Web
Ads, Forum/Bulletin Boards" "MinimalRisk" "text/html" 1 "" "" "0"
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	McAfee WebGateway
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Microsoft ISA Server

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Application type	**Process level metrics**: CPU utilization, memory utilization	Performance Monitoring
WMI	Application type, service mappings	**Process level metrics**: uptime, CPU Utilization, Memory utilization, Read I/O, Write I/O	Performance Monitoring
Syslog(via SNARE)	Application type	**W3C proxy logs**: attributes include Service Instance, Source IP, User, Destination IP, Destination Port, Service Instance, Sent Bytes, Received Bytes, Connection Duration, HTTP User Agent, HTTP Referrer, HTTP Version, HTTP Method, HTTP Status Code, URL, Source interface, Destination interface, Proxy action	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "isa server" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- WMI
- Syslog

SNMP

- Enabling SNMP on Windows Server 2003
- Enabling SNMP on Windows 7 or Windows Server 2008 R2

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you must make sure that the SNMP Management tool has been enabled for your device.

1. In the **Start** menu, go to **Administrative Tools > Services**.
2. Go to **Control Panel > Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Select **Management and Monitoring Tools** and click **Details**.
   Make sure that **Simple Network Management Tool** is selected.
   If it isn't selected, select it, and then click **Next** to install.
5. Go to **Start > Administrative Tools > Services**.
6. Select and open **SNMP Service**.
7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts**.
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service**.

Enabling SNMP on Windows 7 or Windows Server 2008 R2

SNMP is typically enabled by default on Windows Server 2008, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you should check that SNMP Services have been enabled for your server.

1. Log in to the Windows 2008 Server where you want to enable SNMP as an administrator.
2. In the **Start** menu, select **Control Panel**.
3. Under **Programs**, click **Turn Windows features on/off**.
4. Under **Features**, see if **SNMP Services** is installed.
   If not, click **Add Feature**, then select **SMNP Service** and click **Next** to install the service.
5. In the **Server Manager** window, go to **Services > SNMP Services**.
6. Select and open **SNMP Service**.
7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts.**
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.

13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service**.

WMI

Configuring WMI on your device so FortiSIEM can discover and monitor it requires you to create a user who has access to WMI objects on the device. There are two ways to do this:

- Creating a Generic User Who Does Not Belong to the Local Administrator Group
- Creating a User Who Belongs to the Domain Administrator Group

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

- Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group
- Enable DCOM Permissions for the Monitoring Account

Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **Add User**.
3. Create a user.
4. Go to **Groups**, right-click **Distributed COM Users**, and then click **Add to group**.
5. In the **Distributed COM Users Properties** dialog, click **Add**.
6. Find the user you created, and then click **OK**.
   This is the account you must use to set up the Performance Monitor Users group permissions.
7. Click **OK** in the Distributed COM Users Properties dialog, and then close the Computer Management dialog.
8. Repeat steps 4 through 7 for the Performance Monitor Users group.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions,** click **EditDefault**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.

12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

- Enable Remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group
- Enable the Monitoring Account to Access the Monitored Device
- Enable DCOM Permissions for the Monitoring Account
- Enable Account Privileges in WMI
- Allow WMI to Connect Through the Windows Firewall (Windows 2003)
- Allow WMI through Windows Firewall (Windows Server 2008, 2012)

Enable Remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Pane > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user for the @accelops.com domain.
   For example, **YJTEST@accelops.com.**
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties.**
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2.**
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced.**
8. Select the user you created for the monitoring account, and then click **Edit.**
9. In the **Apply onto** menu, select **This namespace and subnamespaces.**
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and the click **OK.**

You can configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

Use the Windows Agent Installation Guide to configure sending syslog from your device to FortiSIEM.

Sample Microsoft ISA Server Syslog

```
<13>Mar  6 20:56:03 ISA.test.local ISAWebLog    0    192.168.69.9    anonymous
Mozilla/5.0 (Windows; U; Windows NT 5.2; en-GB; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12
 Y    2011-03-05    21:33:55    w3proxy    ISA    -    212.58.246.82    212.58.246.82    80
  156    636    634    http    TCP    GET    http://212.58.246.82/rss/newsonline_uk_
edition/front_page/rss.xml    text/html; charset=iso-8859-1    Inet    301    0x41200100
Local Machine    Req ID: 07c10445; Compression: client=No, server=No, compress rate=0%
decompress rate=0%    Local Host    External    0x400    Allowed    2011-03-05 21:33:55    -
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Oracle Cloud Access Security Broker (CASB)

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Log

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
API		Risk Events, Risk Alerts and Policy Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Oracle-CASB-" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 3 event types defined.

Rules

There are no specific rules available for Oracle CASB.

Reports

There are no specific reports available for Oracle CASB. You can view all Oracle events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Oracle-CASB-".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

Setup in FortiSIEM

FortiSIEM processes events from this via the Oracle CASB API. Configure and obtain from the Oracle CASB Portal, the access key and secret from the API before proceeding.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Oracle CASB
Access Protocol	Oracle CASB API
Pull Interval	5 minutes
Access Key	The access key for your Oracle CASB instance.

Settings	Description
Secret Key	The secret key for Oracle CASB instance.
Confirm Secret Key	Input the same secret key as above for verification.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Oracle CASB.
5. To see the jobs associated with Oracle CASB, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "CASB" in the search box.

Sample Log

```
<![CDATA[[FSM-OracleCASB-riskevent] [1] {"id":"aa1nhj35-6d84-3f5a-a9b5-
3e1509bad324","uri":"/v1/events/riskevent?eventId=aa1eab35-6d84-3f5a-a9b5-
3e1509bad324&applicationInstanceId;=5786ed4c-3527-413d-8j19-
da93d0f065c8","appname":"AWS","appinstance":"awse2e_01","appinstanceid":"64909d3d-3855-5de1-
49ed-6452ae9f6365","snapdate":"2017-10-25","title":"DeleteSecurityGroup action in EC2
SecurityGroup \"SecurityGroup\"","additionalDetails":[{"Details":
[{"name":"Actor","value":"funct_test_nonservice"},{"name":"Resource type","value":"EC2
SecurityGroup"},{"name":"Group","value":"SecurityGroup"},{"name":"Resource name","value":"
[JKSecurityGroup]"},{"name":"Action","value":"DeleteSecurityGroup"},{"name":"Policy alert
name","value":"EC2 - Instances Network Routes Network ACL VPN and Security Group changes"},
{"name":"Occurred","value":"2017-10-25T17:17:29Z"},
{"name":"recommendationkey","value":"AWS~PolicyAlert~ec2deletesecuritygroup"}],"Logdata":"
{\"requestParameters\" :{\"groupName\" :\"SecurityGroup\"},\"responseElements\" :{\"_
return\" :true},\"eventVersion\" :\"1.05\",\"eventTime\" :\"2017-10-
25T17:17:29Z\",\"eventSource\" :\"ec2.amazonaws.com\",\"eventName\"
:\"DeleteSecurityGroup\",\"awsRegion\" :\"us-east-1\",\"sourceIPAddress\"
:\"54.191.225.186\",\"userAgent\" :\"aws-sdk-java/1.10.54 Linux/3.13.0-35-generic Java_
HotSpot(TM)_64-Bit_Server_VM/25.60-b23/1.8.0_60\",\"userIdentity\" :{\"type\"
:\"IAMUser\",\"principalId\" :\"BGHAJVECQI6KOIYZMM42A\",\"arn\"
:\"arn:aws:iam::141111463221:user/funct_test_nonservice\",\"accountId\"
:\"141111462111\",\"accessKeyId\" :\"BJKFJ4J6OYTZDBHN3KA\",\"userName\" :\"funct_test_
nonservice\"},\"requestID\" :\"bc44cd99-fac7-4e6c-8868-382c26fc95ee\",\"eventID\"
:\"664d6fa8-8bdf-4bda-af5c-55d447620a78\"}"}],"category":"Policy
alert","priority":"High","status":"Open","createdon":"2017-10-
25T17:33:55.000Z","realeventtime":"2017-10-25T17:17:29.000Z"}]]>
```

Proofpoint

- What is Discovered and Monitored
- Event Types
- Rules
- Reports

- Configuration
- Sample Log

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
API		Alert Event logs	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Proofpoint-" to see the event types associated with this device. In FortiSIEM 6.2.0, there are 2 event types defined.

Rules

There are no specific rules available for Proofpoint.

Reports

There are no specific reports available for Proofpoint. You can view all Proofpoint events by taking the following steps.

1. From the **ANALYTICS** page, click in the **Edit Filters and Time Range** field.
2. Under **Filter**, select **Event Attribute**.
3. In the **Attribute** field, select/enter "Event Type".
4. In the **Operator** field, select "CONTAIN".
5. In the **Value** field, enter "Proofpoint".
6. (Optional) Click **Save** to save the search parameters for future related searches.
7. Click **Apply & Run**.

Configuration

- API
- Setup in FortiSIEM

API

FortiSIEM processes events from Proofpoint via the ProofPoint API. Configure in and obtain from the Proofpoint Portal the Principal and Secret from the API. FortiSIEM uses the ProofPoint API defined here.

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
    a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
    b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Proofpoint Proofpoint
Access Protocol	Proofpoint SIEM API
Pull Interval	5 minutes
Principal	The access key for your Proofpoint instance.
Secret	The secret for Proofpoint instance.
Confirm Secret	Input the same secret as above for verification.
Organization	Choose the Organization the instance belongs to.
Description	Description about the instance.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
    a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
    b. Select the name of your credential from the **Credentials** drop-down list.
    c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Proofpoint.
5. To see the jobs associated with Proofpoint, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Proofpoint" in the search box.

Sample Log

```
<! [CDATA[2018-09-29 17:56:00 [FSM-PROOFPOINT] [1] [clicksPermitted]:
{"campaignId":"46e01b8a-c899-404d-bcd9-
189bb393d1a7","classification":"MALWARE","clickIP":"192.0.2.1","clickTime":"2016-06-
24T19:17:44.000Z","messageID":"8c6cfedd-3050-4d65-8c09-
c5f65c38da81","recipient":"bruce.wayne@pharmtech.zz","sender":"9facbf452def2d7efc5b5c48cdb83
7fa@badguy.zz","senderIP":"192.0.2.255","threatID":"61f7622167144dba5e3ae4480eeee78b23d66f7d
fed970cfc3d086cc0dabdf50","threatTime":"2016-06-
24T19:17:46.000Z","threatURL":"https://threatinsight.proofpoint.com/#/73aa0499-dfc8-75eb-
1de8-
a471b24a2e75/threat/u/61f7622167144dba5e3ae4480eeee78b23d66f7dfed970cfc3d086cc0dabdf50","url
":"http://badguy.zz/","userAgent":"Mozilla/5.0
(WindowsNT6.1;WOW64;rv:27.0)Gecko/20100101Firefox/27.0"}]
```

Squid Web Proxy

- What is Discovered and Monitored
- Event Types
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, Interfaces, Serial number	CPU utilization, Memory utilization	Performance Monitoring
Syslog		**Proxy traffic:** attributes include Source IP, Destination IP, Destination Name, Destination Port, URL, Web category, Proxy action, HTTP User Agent, HTTP Referrer, HTTP Version, HTTP Method, HTTP Status Code, Sent Bytes, Received Bytes, Connection Duration	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "squid" to see the event types associated with this device.

Configuration

- SNMP
- Syslog
- Configure syslogd (or rsyslogd) to Forward the Logs to FortiSIEM
- Sample Parsed Squid Syslog Messages

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Syslog

1. Add the following line to the `logformat` section in `/etc/squid/squid.conf` based of your version of Squid.

   For Squid versions earlier than 4.1.1:

```
logformat PHCombined %>a %>p %<A %la %lp %tr %ul %ui %un %us %ue [%tl] %rm "%ru"
HTTP/%rv %Hs %<st %>st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
```

For Squid version 4.1.1 and later:

```
logformat PHCombined %>a %>p %<A %la %lp %tr %ul %ui %un [%tl] %rm "%ru" HTTP/%rv %Hs
%<st %>st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
```

2. Add the following line to the `access_log` section in `/etc/squid/squid.conf`.

   ```
   access_log syslog:LOG_LOCAL4 PHCombined
   ```

3. Restart Squid.

Configure syslogd (or rsyslogd) to Forward the Logs to FortiSIEM

1. Modify `/etc/syslog.conf` (`/etc/rsyslog.conf` if running `rsyslog`).

   ```
   Local4.*
   ```

   ```
   @<FortiSIEMIp>
   ```

2. Restart syslogd (or rsyslogd).

Sample Parsed Squid Syslog Messages

- Squid on Linux with syslog Locally to Forward to FortiSIEM
- Squid on Linux with syslog-ng Locally to Forward to FortiSIEM
- Squid on Linux with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM
- Squid on Linux with syslog-ng Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM
- Squid on Solaris with syslog Locally to Forward to FortiSIEM
- Squid on Solaris with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM

Squid on Linux with syslog Locally to Forward to FortiSIEM

```
<166>squid[28988]: 192.168.25.15 51734 65.54.87.157 172.16.10.40 3128 5989 - - - - -
[22/Apr/2011:17:17:46 -0700] GET "http://col.stj.s-msn.com/br/sc/js/jquery/jquery-
1.4.2.min.js" HTTP/1.1 200 26141 407 "http://www.msn.com/" "Mozilla/5.0 (Windows; U; Windows
NT 6.1; en-US; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16" TCP_MISS:DIRECT
```

Squid on Linux with syslog-ng Locally to Forward to FortiSIEM

```
<166>Oct 20 09:21:54 QA-V-CentOS-Syslog-ng squid[7082]: 192.168.20.42 1107 74.125.19.100
172.16.10.34 3128 291 - - - - - [20/Oct/2009:09:21:54 -0700] GET
"http://clients1.google.com/generate_204" HTTP/1.1 204 387 603 "http://www.google.com/"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR
3.0.4506.2152; .NET CLR 3.5.30729)" TCP_MISS:DIRECT
```

Squid on Linux with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM

```
<166>Oct 20 10:21:42 172.16.10.40 squid[26033]: 192.168.20.42 1121 66.235.132.121
172.16.10.40 3128 117 - - - - - [20/Oct/2009:12:05:49 \-0700|] GET
```

```
"http://metrics.sun.com/b/ss/sunglobal,suncom,sunstruppdev/1/H.14/s21779365053734?" HTTP/1.1
200 746 1177 "http://www.sun.com/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET
CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" TCP_MISS:DIRECT
```

Squid on Linux with syslog-ng locally and forward to syslog-ng remotely to forward to FortiSIEM

```
<166>Oct 20 12:44:12 172.16.10.40 squid[26033]: 192.168.20.42 1125 64.213.38.80 172.16.10.40
3128 117 - - - - - [20/Oct/2009:12:44:12 -0700] GET "http://www-cdn.sun.com/images/hp5/hp5b_
enterprise_10-19-09.jpg" HTTP/1.1 200 12271 520 "http://www.sun.com/" "Mozilla/4.0
(compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)" TCP_MISS:DIRECT
```

Squid on Solaris with syslog Locally to Forward to FortiSIEM

```
<166>May  6 17:55:48 squid[1773]: [ID 702911 local4.info] 192.168.20.39 1715 72.14.223.18
172.16.10.6 3128 674 - - - - - [06/May/2008:17:55:48 -0700] GET
"http://mail.google.com/mail/?" HTTP/1.1 302 1061 568 "http://www.google.com/" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-US; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14" TCP_
MISS:DIRECT
```

Squid on Solaris with syslog Locally and Forward to syslog-ng Remotely to Forward to FortiSIEM

```
<166>Oct 20 13:02:19 172.16.10.6 squid[687]: [ID 702911 local4.info] 192.168.20.42 1112
208.92.236.184 172.16.10.6 3128 201 - - - - - [20/Oct/2009:13:02:19 -0700] GET
"http://m.webtrends.com/dcs4f6vsz99k7mayiw2jzupyr_1s2e/dcs.gif?" HTTP/1.1 200 685 1604
"http://www.microsoft.com/en/us/default.aspx" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" TCP_MISS:DIRECT
```

SSH Comm Security CryptoAuditor

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	15 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "CryptoAuditor-" in the main content panel **Search...** field to see the event types associated with this device. .

Sample Event Type:

```
<189>Jun 24 15:43:01 auditor ssh-auditor[4067]:
CEF:0|SSH|CryptoAuditor|1.6.0|4201|Connection_received|1|rt=Jun 26 2015 07:48:24
SshAuditorSrc=10.1.78.8 spt=34453 SshAuditorDst=10.1.78.8 dpt=10022 SshAuditorSessionId=21
SshAuditorUsername=testuser SshAuditorRemoteusername=testuser
SshAuditorProtocolsessionId=C089C55D9ADE0A4F901917D69B46B01223A02B70 SshAuditorVirtualLAN=0
cs1=source connection cs1Label=Text
```

```
<189>Jun 24 15:43:01 auditor ssh-auditor[4067]:
CEF:0|SSH|CryptoAuditor|1.6.0|4201|Connection_received|rt=Jun 26 2015 07:48:24
SshAuditorSrc=10.1.78.8 spt=34453 SshAuditorDst=10.1.78.8 dpt=10022 SshAuditorSessionId=21
SshAuditorUsername=testuser SshAuditorRemoteusername=testuser
SshAuditorProtocolsessionId=C089C55D9ADE0A4F901917D69B46B01223A02B70 SshAuditorVirtualLAN=0
cs1=source connection cs1Label=Text
```

Rules

There are no specific rules but generic rules for Generic Servers apply.

Reports

There are no specific reports but generic rules for Generic Servers apply.

Configuration

Configure SSH Comm Security CryptoAuditor to send syslog on port 514 to FortiSIEM.

Websense Web Filter

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Parsed Websense Web Filter Syslog Message
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Syslog		**Parsed event attributes**: include Source IP, Destination Name, Destination URL, HTTP Method, HTTP User agent, HTTP Status Code, HTTP Content Type, Blocked Reason, Website category, HTTP Disposition, Sent Bytes, Recv Bytes, Duration, File Type etc	Security Monitoring and compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "websense_web" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

FortiSIEM integrates with Websense Web Filter via syslog sent in the SIEM integration format as described in the Websense SEIM guide. See the instructions on how to install a Websense Multiplexer that integrates with Websense Policy server and creates syslog for consumption by SIEM products such as FortiSIEM.

Sample Parsed Websense Web Filter Syslog Message

```
<159>Feb 28 14:25:32 10.203.28.21 vendor=Websense product=Security product_version=7.7.0
action=permitted severity=1 category=153
user=- src_host=10.64.134.74 src_port=62189 dst_host=mail.google.com dst_ip=74.125.224.53
dst_port=443 bytes_out=197 bytes_in=76
http_response=200 http_method=CONNECT http_content_type= -
http_user_agent=Mozilla/5.0_(Windows;_U;_Windows_NT_6.1;_enUS;_rv:1.9.2.23)_Gecko/20110920_
Firefox/3.6.23
http_proxy_status_code=200 reason=- disposition=1034 policy=- role=8 duration=0
url=https://mail.google.com
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Websense Web Security
Access Protocol	JDBC
Log Server IP	IP of the log server
Pull Interval	5 minutes
Port	1433
Log Database	wslogdb70_1
URL Database	wslogdb70
URL Category Database	wslogdb70
Disposition Database	wslogdb70
User Name	Name used to access the database

Security Orchestration (SOAR)

FortiSIEM supports these Security Orchestration, Automation and Response (SOAR) applications.

- Fortinet FortiSOAR

Fortinet FortiSOAR

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Log Format	Used for
Syslog	CEF	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortisoar" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configuring FortiSOAR for Syslog Forwarding

To configure FortiSOAR to forward syslog to FortiSIEM, take the following steps:

Note: It is recommended that you refer to the most current FortiSOAR Administration Guide for the latest configuration steps. Configuration steps here from the 7.0.0 FortiSOAR Administration Guide.

1. From FortiSOAR, navigate to **Settings > Configuration > Log Forwarding**.
2. Check the **Enable Log Forwarding** checkbox.
3. Configure the Syslog Server Details as follows.

Field	Input
Configuration Name	Input "FortiSIEM".
Server	Input the IP address or FQDN of the FortiSIEM Collector.
Protocol	Select **UDP**.
Port	Input "514".
Choose Log Types to Forward	Select all options.
Specify Audit Log Detail Level	Select **Detailed.**
Configure Audit Log Forward Rules	Select what you want logged to FortiSIEM.

4. Click **Save**.

Servers and Workstations

FortiSIEM supports these servers and workstations for discovery and monitoring.

- Apple MacOS Servers and Workstations
- HP UX Server
- IBM AIX Server
- IBM OS400 Server
- Linux Server
- Microsoft Windows Server
- QNAP Turbo NAS
- Sun Solaris Server

Apple MacOS Servers and Workstations

FortiSIEM Support added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Apple

Product: Apple MacOS

Product Information: https://www.apple.com/macos/, https://www.apple.com/macos/server/

- Log Information
- Event Types

Log Information

Log Collection Method	Purpose
Syslog	Security and Compliance

Event Types

In 6.3.1, there are 17 event types.

HP UX Server

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	Hardware **(cpu details, memory**)	**Memory paging rate, Disk I/O utilization**	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "hp-ux" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "hp_ux" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- SNMP v1 and v2c
- SSH

SNMP v1 and v2c

1. Make sure that snmp libraries are installed. FortiSIEM has been tested to work with the default HP UX package that comes with snmpd preinstalled.
2. Start snmpd deamon with the default configuration by issuing `/etc/init.d/snmpd restart`.
3. Make sure that snmpd is running.

SSH

1. Make sure that the `vmstat` and `iostat` commands are available. If not, install these libraries.
2. Create a user account that can issue `vmstat` and `iostat` commands. FortiSIEM will use that user account to login to the server.

Settings for Access Credentials

- SNMP, Telnet, and SSH Access Credentials for All Devices
- LDAP, LDAPS, LDAP Start TLS / Open LDAP Access Credentials for All Devices
- LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

SNMP, Telnet, and SSH Access Credentials for All Devices

See Access Credentials.

LDAP, LDAPS, LDAP Start TLS / Open LDAP Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	HP HPUX
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	OpenLDAP
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
Password Config	See Password Configuration
User Name	Name of the user able to access this system

Settings	Value
Password	Password of the user able to access this system

LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	HP HPUX
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	Microsoft Active Directory
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

IBM AIX Server

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	Hardware **(cpu details, memory**)	**Memory paging rate, Disk I/O utilization**	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "ibm_aix" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP v1 and v2c
- SSH
- Syslog

SNMP v1 and v2c

1. Make sure that snmp libraries are installed. Accelops has been tested to work with the default AIX package that comes with snmpd preinstalled.
2. Start snmpd deamon with the default configuration by issuing `/etc/init.d/snmpd restart`.
3. Make sure that snmpd is running.

SSH

1. Make sure that the `vmstat` and `iostat` commands are available. If not, install these libraries.
2. Create a user account that can issue `vmstat` and `iostat` commands. FortiSIEM will use that user account to log in to the server.

Syslog

1. Makes sure that `/etc/syslog.conf` contains a `*.*` entry and points to a log file.

   ```
   . @<SENSORIPADDRESS>
   ```

2. Refresh syslogd.

   ```
   # refresh -s syslogd
   ```

Settings for Access Credentials

- SNMP, Telnet, and SSH Access Credentials for All Devices
- LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices
- LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

SNMP, Telnet, and SSH Access Credentials for All Devices

See Access Credentials.

LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices

Settings	Value
Name	<set name>

Settings	Value
Device Type	IBM AIX
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	OpenLDAP
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	IBM AIX
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	Microsoft Active Directory
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

IBM OS400 Server

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Parsed IBM OS400 Syslog Messages

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog		General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "os400" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

FortiSIEM parses IBM OS 400 logs received via the PowerTech Agent as described here. The PowerTech agent sends syslog to FortiSIEM.

Sample Parsed IBM OS400 Syslog Messages

```
Mar 18 17:49:36 ROBINSON CEF :0|PowerTech|Interact|2.0|UNA0603|A File Server transaction was
allowed for user BRENDAN.|2| src =10.0.1.60 dst =10.0.1.180 msg=TYPE:JRN CLS :AUD JJOB
```

```
:QPWFSERVSO JUSER :BRENDAN JNBR :025355 PGM :PLKR108JEL OBJECT : LIBRARY : MEMBER: DETAIL:
OB BRENDAN *FILESRV CRTSTRMFIL QPWFSERVSO LNS0811 000112 00023 /home/BRENDAN/subfolder

Mar 18 17:48:36 ROBINSON CEF :0|PowerTech|Interact|2.0|UNA0604|A File Server transaction was
allowed for user BRENDAN.|2| src =10.0.1.60 dst =10.0.1.180 msg=TYPE:JRN CLS :AUD JJOB
:QPWFSERVSO JUSER :BRENDAN JNBR :025355 PGM :PLKR108JEL OBJECT : LIBRARY : MEMBER: DETAIL:
OB BRENDAN *FILESRV DLTSTRMFIL QPWFSERVSO LNS0811 000112 00025 /home/BRENDAN/BoardReport

Mar 18 17:53:00 ROBINSON CEF :0|PowerTech|Interact|2.0|UNA0703|A System i FTP Client
transaction was allowed for user BRENDAN.|3| src =10.0.1.180 dst =10.0.1.180 msg=TYPE:JRN
CLS :AUD JJOB :QTFTP00149 JUSER :BRENDAN JNBR :029256 PGM :PLKR108JEL OBJECT : LIBRARY :
MEMBER: DETAIL: ST BRENDAN *FTPCLIENT DELETEFILE QTFTP00149 LNS0811 000112 00033
/QSYS.LIB/PAYROLL.LIB/NEVADA.FILE
```

Linux Server

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Swap space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	OS type, Hardware **(cpu details, memory**)	**Memory paging rate, Disk I/O utilization**	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance
Syslog (via FortiSIEM Linux Agent)		File or directory change: User, Type of change, directory or file name	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "linux" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "linux" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports** , search for "linux" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

- SNMP v1 and v2c
- SNMP v3
- SSH
- Syslog Logging
- Basic Linux File Monitoring over Syslog

SNMP v1 and v2c

1. Make sure that snmp libraries are installed. FortiSIEM has been tested to work with net-snmp libraries.
2. Log in to your server with administrative access.
3. Make these modifications to the `/etc/snmp/snmpd.conf` file:
   a. Define the community string for FortiSIEM usage and permit snmp access from FortiSIEM IP.
   b. Allow FortiSIEM read-only access to the `mib-2` tree.
   c. Allow Accelops read-only access to the enterprise MIB: `UCD-SNMP-MIB`.
   d. Open up the entire tree for read-only view.
4. Reduce the logging level to avoid per connection logging which may cause resource issues (see here for more details):
   a. Edit `/etc/sysconfig/snmpd` (on RedHat/CentOS) or `/etc/defaults/snmpd` (on Debian/Ubuntu)
   b. Look for the line that passes the command line options to snmpd. On RedHat Enterprise 6 this looks like:

      ```
      # snmpd command line options
      OPTIONS="-LS0-6d -Lf /dev/null -p /var/run/snmpd.pid"
      ```

   c. Change the range from 0-6 to 0-5:

      ```
      # snmpd command line options
      OPTIONS="-LS0-5d -Lf /dev/null -p /var/run/snmpd.pid"
      ```

5. Restart the snmpd deamon by issuing `/etc/init.d/snmpd restart`.
6. Add the snmpd daemon to start from boot by issuing `chkconfig snmpd on`.
7. Make sure that snmpd is running.

SNMP v3

Configuring rwcommunity/rocommunity or com2sec

1. Log in to your Linux server.
2. Stop SNMP.

   ```
   service snmpd stop
   ```

3. Use vi to edit the `/etc/snmp/snmpd.conf` file.
   Before you edit this file, make sure you have created a backup, as it is very important to have a valid version of this file so the snap daemon has correct credentials.

   ```
   vi /etc/snmp/snmpd.conf
   ```

4. At the end of the file, add this line, substituting your username for `snmpv3user` and removing the `<>` tags: `rouser <snmpv3user>`.
5. Save the file.
6. Use vi to edit the `/var/lib/snmp/snmpd.conf` file.
   Before you edit this file, make sure you have created a backup, as it is very important to have a valid version of this file for the SNMP daemon to function correctly.

   ```
   vi /var/lib/snmp/snmpd.conf
   ```

7. At the end of the file, add this line, entering the username you entered in step 4, and then passwords for that user for MD5 and DES.
   If you want to use SHA or AES, then add those credentials as well.

   ```
   createUser <snmpv3user>        MD5 <snmpv3md5password> DES <snmpv3despassword>
   ```

8. Save the file.
9. Reduce the logging level to avoid per connection logging which may cause resource issues (see here for more details)
   a. Edit `/etc/sysconfig/snmpd` (on RedHat/CentOS) or `/etc/defaults/snmpd` (on Debian/Ubuntu)
   b. Look for the line that passes the command line options to `snmpd`. On RedHat Enterprise 6 this looks like:

      ```
      # snmpd command line options
      OPTIONS="-LS0-6d -Lf /dev/null -p /var/run/snmpd.pid"
      ```

   c. Change the range from 0-6 to 0-5:

      ```
      # snmpd command line options
      OPTIONS="-LS0-5d -Lf /dev/null -p /var/run/snmpd.pid"
      ```

10. Restart SNMP.

    ```
    service snmpd start
    chkconfig auditd on
    ```

11. View the contents of the `/var/lib/snmp/snmpd.conf` file.
    If this works, restarting `snmpd` will have no errors, also the entry that you created under `/var/lib/snmp/snmpd.conf` will be removed:

    ```
    cat /var/lib/snmp/snmpd.conf
    ```

12. Run `snmpwalk -v 3 -u <snmpv3user> -l authpriv <IP> -a MD5 -A <snmpv3md5password> -x DES -X <snmpv3despassword>`
    You will see your `snmpwalk` if this works. If there are any errors, see `net-snmp` for further instructions.

Configuring net-smnp-devel

If you have `net-snmp-devel` on your Linux server/client, follow these steps to configure SNMP v3.

1. Stop SNMP.

   ```
   service snmpd stop
   ```

2. Run `net-snmp-config --create-snmpv3-user -ro -A <MD5passwordhere> -X <DESpasswordhere> -x DES -a MD5 <SNMPUSERNAME>.`
3. Restart SNMP.

   ```
   service snmpd start
   ```

4. Test by following step 10 from above.

SSH

1. Make sure that the `vmstat` and `iostat` commands are available. If not, install these libraries.
2. Create a user account that can issue `vmstat` and `iostat` commands. FortiSIEM will use that user account to log in to the server.

Syslog Logging

Syslog forwarding can be configured on Linux servers to send the logs to FortiSIEM. There are different options regarding syslog configuration, including Syslog over TLS.

There are typically two commonly-used Syslog demons:

- Syslog-ng
- Rsyslog

Basic Syslog-ng Configuration

Follow these steps to enable basic syslog-ng:

1. Add the following line to your syslog-ng configuration:
   `{ udp("Collector IP" port(514));};`
2. Restart the syslog-ng service or reload the configuration.

Additional Syslog-ng Configuration Information and Example

Source options are:

`internal()` means syslog-ng internal log messages.

`system()` means depending on your platform, syslog-ng will automatically collect the common log sources.

Filter functions:

`facility(`*`xx`*`,`*`xx`*`,`*`xx`*`)` allows filtering only the defined log facilities

Here is an example of configuring just authpriv and auth log facilities.
Note: Remember to replace italicized text with your content.

1. Open the `/etc/syslog-ng/syslog-ng.conf` file.
2. Add the following configuration.

```
source fsiem_source {
                internal();
                system();
};
filter fsiem_filter {
    facility(auth, authpriv);
};
destination fsiem_destination {
    udp("<collector_ip>" port(514));
};
log{
    source(fsiem_source);
    filter(fsiem_filter);
    destination(fsiem_destination);
};
```

3. Save the file and restart syslog-ng by running the command:

   `service syslog-ng restart`

   or

   `systemctl restart syslog-ng`

Here is an example of verbose logging, where all log facilities are sent.
Note: Remember to replace italicized text with your content.

1. Open the `/etc/syslog-ng/syslog-ng.conf` file.
2. Add the following configuration.

```
source fsiem_source {
                internal();
                system();
};
destination fsiem_destination {
    udp("<collector_ip>" port(514));
};
log{
    source(fsiem_source);
    destination(fsiem_destination);
};
```

3. Save the file and restart syslog-ng by running the command:

   `service syslog-ng restart`

   or

   `systemctl restart syslog-ng`

Basic Rsyslog Configuration

Follow these steps to enable rsyslog:

1. Add the following lines to your rsyslog configuration:

```
# Send logs to the FortiSIEM Collector
*.* @Collector IP:514
```

2. Restart the rsyslog service or reload the configuration.

   Additional Rsyslog Configuration Information and Example

   Rsyslog has a list of supported facilities, or app subsystems shown here.

Supported Facility/App Subsystem	Description
auth, authpriv	authentication and authorization logs
cron	cron scheduling
daemon	affects a daemon without any special classification (DNS, NTP, etc)
ftp	ftp server events
kern	kernel messages
lpr	printing subsystem
mail	email subsystem
news	Usenet subsystem messages, NNTP, etc...
syslog	internal syslogd server messages
user	user messages (generic)
uucp	UUCP server messages
local0 - local7	local user

Each message has a priority level, listed here from the most important to least important priority.

```
emerg, alert, crit, error, warn, notice, info, debug
```

In the rsyslog conf file, you can reference to log a facility in the format shown here.

```
<facility>.<priority> @<server ip or name>:<server_port>
```

where @ implies UDP and @@ implies TCP, and the italicized text should be replaced with your information.

A wildcard for any facility can be specified with an asterisk (*). For example:

*auth.** means any priority of auth messages are sent to target.

Here is a walk through example to just log authentication messages to FortiSIEM from modifying the rsyslog.conf file (`vi /etc/rsyslog.conf`)
Note: Remember to replace italicized text with your content.

1. Add the following lines to only add audit trails to be sent to the FortiSIEM collector.

   ```
   authpriv.* @<Your_FortiSIEM_Collectors_IP_or_Hostname>:514
   auth.* @<Your_FortiSIEM_Collectors_IP_or_Hostname>:514
   ```

2. Save the file and restart rsyslog using the following command.

   ```
   service rsyslogd restart
   ```

   or

   ```
   systemctl restart rsyslog.service
   ```

3. log into this server or run a `sudo` command to confirm that logs appear in FortiSIEM, and that a CMDB entry is created if it does not already exist.

   For verbose logging for all facilities and priorities, use the following.

   ```
   *.* @<server ip or hostname>:514
   ```

Linux File Monitoring

FortiSIEM has licensed Linux agents that provide additional capabilities, such as custom log forwarding and central management. See the “Linux Agent Installation Guide” for details on this agent.

Settings for Access Credentials

- SNMP Access Credentials for All Devices
- SSH Access Credentials for All Devices

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

SSH Access Credentials for All Devices

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	ssh-generic
Device Type	Generic
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Microsoft Windows Server

Supported OS

- Windows 2003
- Windows 2008 and 2008 R2
- Windows 2012 and 2012 R2
- Windows 2016
- Windows 2019

What is Discovered and Monitored

Metrics in bold are unique to Microsoft Windows Server monitoring.

Installed Software Monitored via SNMP

Although information about installed software is available via both SNMP and WMI, FortiSIEM uses SNMP to obtain installed software information to avoid an issue in Microsoft's WMI implementation for the Win32_Product WMI class - see Microsoft KB 974524 article for more information. Because of this bug, WMI calls to the Win32_Product class create many unnecessary Windows event log messages indicating that the Windows Installer has reconfigured all installed applications.

Winexe execution and its effect

FortiSIEM uses the **winexe** command during discovery and monitoring of Windows servers for the following purposes

1. Windows domain controller diagnostic (dcdiag) and replication monitoring (repadmin /replsummary)
2. HyperV Performance Monitoring
3. Windows Custom performance monitoring – to run a command (e.g. powershell) remotely on windows systems

Note: Running the `winexe` command remotely will automatically install the `winexesvc` command on the windows server.

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, **installed software**,	Uptime, Overall CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, **Installed Software change**, Running process	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
	running processes, open TCP/UDP ports)	CPU/memory utilization, Running process start/stop, **TCP/UDP port up/down**	
SNMP	Vendor specific server hardware (hardware model, hardware serial number, fans, power supply, disk, raid battery). Currently supported vendors include HP and Dell	Hardware module status - fan, power supply, thermal status, battery, disk, memory . Currently supported vendors include HP and Dell	
WMI	Win32_ComputerSystem: Host name, OS Win32_WindowsProductActivation: OS Serial Number Win32_OperatingSystem: Memory, Uptime Win32_BIOS: Bios Win32_Processor: CPU Win32_LogicalDisk: Disk info Win32_NetworkAdapterConfiguration: network interface Win32_Service: Services Win32_Process: Running processes Win32_QuickFixEngineering: Installed Patches	Win32_OperatingSystem: Uptime Win32_PerfRawData_PerfOS_Processor: Detailed CPU utilization Win32_PerfRawData_PerfOS_Memory: Memory utilization, paging/swapping metrics Win32_LogicalDisk: Disk space utilization Win32_PerfRawData_PerfOS_PagingFile: Paging file utilization Win32_PerfRawData_PerfDisk_LogicalDisk: Disk I/O metrics Win32_PerfRawData_Tcpip_NetworkInterface: Network Interface utilization Win32_Service: Running process uptime, start/stop status Win32_Process, Win32_PerfRawData_PerfProc_Process: Process CPU/memory/I/O utilization	Performance Monitoring
WMI		Security, Application and System Event Logs including logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
Snare agent		Security, Application and System Event Logs including logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
Correlog agent		Security, Application and System Event Logs ncluding logon, file/folder edits, network traffic (Win32_NTLogEvent)	Security and Compliance
FortiSIEM Agent		Security, Application and System Event Logs, DNS, DHCP, IIS, DFS logs, Custom log files, File Integrity Monitoring, Registry Change Monitoring, Installed Software Change Monitoring, WMI and Powershell output monitoring	Security and Compliance

Windows Server Monitoring Summary

Log Collection Features	WMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Security, Application, System Event Logs	Yes	Yes
File/Folder Edits	Yes	Yes
File Integrity Monitoring (FIM)	No	Yes
IIS Audit Logs	No	Yes
DNS Analytical Logs	No	Yes
Detailed DHCP Audit Logging	No	Yes
Support for all Windows Log Channels	No	Yes
Custom Log Sources	No	Yes
Windows Event Collector (WEC) Support	No	Yes
Sysmon Event Support	No	Yes
Registry Change Monitoring	No	Yes
Installed Software Change Monitoring	No	Yes
WMI and Powershell Output Monitoring	No	Yes
Supports UEBA Telemetry Data	No	Yes

Performance Features	WMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Scalable for Large Environments	No	Yes
EPS Performance	100 EPS max	5K EPS
Performance Monitoring	Yes	No

Administrative Features	WMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Simplified Network Policies	No (TCP 135,1024-65535 inbound)	Yes (443 outbound)
Requires Domain or Local Service Account	Yes	No

Administrative Features	WMI (Windows Mgmt Instrumentation)	FortiSIEM Windows Agent
Requires Install on Server or Workstation	No	Yes
FIPS Compliant Capable	No	Yes
Log Buffering Upon Connectivity Loss	No	Yes
Supports On and Off Network Monitoring	No	Yes
Secure Log Transmission	Yes	Yes

Event Types

In **ADMIN > Device Support > Event Types**, search for "windows server" to see the event types associated with this application or device.

Rules

In **RESOURCES > Rules**, search for "windows server" in the main content panel **Search...** field to see the rules associated with this application or device.

Reports

In **RESOURCES > Reports**, search for "windows server" in the main content panel **Search...** field to see the reports associated with this application or device.

Configuration

- WinRM Configurations
- SNMP Configurations
- WMI Configurations
- Windows Agent Configurations
- Syslog Configurations
- Configuring the Security Audit Logging Policy
- Configuring the File Auditing Policy
- Disabling Audit Token Right Adjusted Success Events
- Configuring Print Log

WinRM Configurations

WinRM is used for some FortiSIEM Remediation actions. If Windows Remediation actions are not used in FortiSIEM, this configuration step is not required.

Enable WinRM and set authentication

Use the commands below to enable WinRM and set authentication on the target Windows Servers:

1. To configure Windows Server:

   ```
   winrm quickconfig
   winrm set winrm/config/service/auth ‘@{Basic="true"}’
   winrm set winrm/config/service ‘@{AllowUnencrypted="true"}’
   winrm enumerate winrm/config/listener
   ```

   Notes:

   - If HTTPS is not enabled, then open Windows PowerShell console as an administrator, and run the following commands.

   ```
   New-SelfSignedCertificate -Subject 'CN=<windows host name>' -TextExtension
   '2.5.29.37={text}1.3.6.1.5.5.7.3.1'
   winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="<windows
   host name>"; CertificateThumbprint="<thumbprint received by New-Self Signed
   Certificate>"}
   winrm quickconfig -transport:https
   winrm enumerate winrm/config/listener
   ```

   - Single quotes are needed for Windows 2016 and later.
2. To configure FortiSIEM Client (Super or Collector):

   ```
   pip install pywinrm
   ```

SNMP Configurations

- Enabling SNMP on Windows Server 2012R2, Server 2016, Server 2019
- Enabling SNMP on Windows 7 or Windows Server 2008 R2
- Enabling SNMP on Windows Server 2003

Enabling SNMP on Windows Server 2012R2, Server 2016, Server 2019

SNMP is typically enabled by default on Windows Server 2012R2, Server 2016, and Server 2019. But you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First, you should check that SNMP Services have been enabled for your server.

1. Log in to the Windows 2016 Server where you want to enable SNMP as an administrator.
2. In the **Start** menu, select **Control Panel**.
3. Under **Programs,** click **Turn Windows features on/off**.
4. The **Add Roles and Features Wizard** will open automatically.
5. Select **Role-based** or **feature-based installation**. Click **Next** until the **Features** option appears.
6. Under **Features**, see if **SNMP Services** is installed.
   If not, check the checkbox before the **SNMP Service** and click **Next** to install the service.
7. From the **Start** menu, select **Services**. Go to **Services > SNMP Services**.
8. Select and open **SNMP Service**.
9. Click the **Security** tab.
10. Select **Send authentication trap**.
11. Under **Accepted communities**, make sure there is an entry for public that is set to read-only.

12. Select **Accept SNMP packets** from these hosts.
13. Click **Add**.
14. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
15. Click **Add**.
16. Click **Apply**.
17. Under **SNMP Service**, click **Restart service**.
18. Navigate to **Control Panel > Windows Firewall**.
19. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
20. Select **SNMP Service**, and the click **OK**.

Enabling SNMP on Windows 7 or Windows Server 2008 R2

SNMP is typically enabled by default on Windows Server 2008, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you should check that SNMP Services have been enabled for your server.

1. Log in to the Windows 2008 Server where you want to enable SNMP as an administrator.
2. In the **Start** menu, select **Control Panel**.
3. Under **Programs**, click **Turn Windows features on/off**.
4. Under **Features**, see if **SNMP Services** is installed.
   If not, click **Add Feature**, then select **SMNP Service** and click **Next** to install the service.
5. In the **Server Manager** window, go to **Services > SNMP Services**.
6. Select and open **SNMP Service**.
7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts**.
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service**.
16. Navigate to **Control Panel > Windows Firewall**.
17. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
18. Select **SNMP Service**, and the click **OK**.

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you must still add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you must make sure that the SNMP Management tool has been enabled for your device.

1. In the **Start** menu, go to **Administrative Tools > Services**.
2. Go to **Control Panel > Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Select **Management and Monitoring Tools** and click **Details**.
   Make sure that **Simple Network Management Tool** is selected.
   If it isn't selected, select it, and then click **Next** to install.
5. Go to **Start > Administrative Tools > Services**.

6. Select and open **SNMP Service**.
7. Click the **Security** tab.
8. Select **Send authentication trap**.
9. Under **Accepted communities**, make sure there is an entry for **public** that is set to **read-only**.
10. Select **Accept SNMP packets from these hosts**.
11. Click **Add**.
12. Enter the **IP address** for your FortiSIEM virtual appliance that will access your device over SNMP.
13. Click **Add**.
14. Click **Apply**.
15. Under **SNMP Service**, click **Restart service.**
16. Navigate to **Control Panel > Windows Firewall**.
17. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
18. Select **SNMP Service**, and the click **OK.**

WMI Configurations

- WMI Configuration for Windows 2012, 2012R2, 2016, 2019
- WMI Configurations for Windows 2008 and 2008R2

WMI Configuration for Windows 2012, 2012R2, 2016, 2019

To configure WMI on your device so that FortiSIEM can discover and monitor it, you must create a user who has access to WMI objects on the device. There are two ways to do this:

- Creating a Generic User Who Does Not Belong to the Local Administrator Group
- Creating a User Who Belongs to the Domain Administrator Group
- Differences Between Administrator and Non-Administrator Account

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Step 1. Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
2. Right-click **Users** and select **New User**.
3. Create a user.
4. Select this user and right-click to select **Properties > Member of** tab.
5. Click **Add > Advanced > Find Now**.
6. Select and add the following groups:
   Note: To select multiple groups, hold down the **CTRL** key and click the desired groups.
   - **Distributed COM Users** group.
   - **Performance Monitor Users** group.
   - **Remote Desktop Users** group.
7. Click **OK** to save.

Step 2. Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services > Computers > My Computer**.
2. Right-click **My Computer**, and then **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **Edit Default**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in Step 1.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow for Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow for Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in Step 1.
14. Click **OK**.

Step 3. See the sections on Enabling WMI Privileges and Allowing WMI Access through the Windows Firewall in the Domain Admin User set up instructions for the remaining steps to configure WMI.

Step 4. Configuring Log Monitoring for Non-Administrative User

To configure the non-administrative user to monitor windows event logs, follow the steps below:

1. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers (Computer Management > Local Users and Groups** for servers that are not a domain controller).
2. Right-click the non-admin user and select **Properties**.
3. Select the **Member of** tab.
4. Select the group **Event Log Reader** and click **Add**.
5. Click **Apply**.
6. Click **OK** to complete the configuration.
7. The following groups should be applied to the user:
   - **Distributed COM Users**
   - **Domain Users**
   - **Event Log Reader**

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Step 1. Enable remote WMI requests by adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start > Control Pane > Administrative Tools > Active Directory Users and Computers > Users**.
2. Right-click **Users** and select **New > User**.
3. Create a user for the `@accelops.com` domain.
   For example, `YJTEST@accelops.com`.
4. Right-click **Domain Admins** in **Users** and select **Properties.**
5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. Click **Advanced > Find Now**, add the **Administrator** and the user which you created in Step 3.
7. Click **OK** to close the **User** select dialog.
8. Click **OK** to close the **Domain Admins Properties** dialog.

Step 2. Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **COM Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that the user has the permission **Allow** for both **Local Access** and **Remote Access**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in Step 1.
8. Click **OK**.
9. In the **COM Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission Allow for **Local Launch**, Remote Launch, Local Activation, and Remote Activation. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in Step 1.
11. In the **COM Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
12. Find the user you created for the monitoring account, and make sure that user has the permission Allow for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**. If the **Distributed COM Users** group and **Performance Monitor Users** group are not present, then click **Add** to add these two groups as described in Step 1.
13. Click **OK**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties.**
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2.**

5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission Allow for **Enable Account** and **Remote Enable**. If the user is not present, then click **Add** to add the user you created.
7. Click **Advanced**.
8. Select the user you created for the monitoring account, and then click **Edit**.
9. In the **Applies onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the **Permission Entry** for **CIMV2** dialog.
11. Click **OK** to close the **Advanced Security Settings** for **CIMV2** dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services**.
13. Select **Windows Management Instrumentation**, and then click **Restart**.

Allow WMI through Windows Firewall (Windows Server 2012, 2016 and 2019)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and the click **OK**. You can configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Differences Between Administrator and Non-Administrator Account

Windows allows certain WMI classes to be pulled only via Administrator account. The following table shows this clearly.

WMI Class	Administrator	Non-Administrator
Win32_BIOS	Yes	No
Win32_ComputerSystem	Yes	Yes
Win32_LogicalDisk	Yes	No
Win32_NetworkAdapter	Yes	Yes
Win32_NetworkAdapterConfiguration	Yes	Yes
Win32_NTLogEvent	Yes	Yes
Win32_OperatingSystem	Yes	Yes
Win32_Process	Yes	Yes
Win32_Processor	Yes	Yes
Win32_Product	Yes	Yes
Win32_QuickFixEngineering	Yes	No
Win32_Service	Yes	No
Win32_UserAccount	Yes	No
win32_Volume	Yes	Yes
Win32_PerfFormattedData_DHCPServer_DHCPServer	Yes	Yes

WMI Class	Administrator	Non-Administrator
Win32_PerfFormattedData_DNS_DNS	Yes	Yes
Win32_PerfFormattedData_W3SVC_WebService	Yes	Yes
Win32_PerfRawData_DirectoryServices_DirectoryServices	Yes	Yes
Win32_PerfRawData_NTDS_NTDS	Yes	Yes
Win32_PerfRawData_PerfDisk_LogicalDisk	Yes	Yes
Win32_PerfRawData_PerfDisk_PhysicalDisk	Yes	Yes
Win32_PerfRawData_PerfOS_Memory	Yes	Yes
Win32_PerfRawData_PerfOS_PagingFile	Yes	Yes
Win32_PerfRawData_PerfOS_Processor	Yes	Yes
Win32_PerfRawData_PerfProc_Process	Yes	Yes
Win32_PerfRawData_Tcpip_NetworkInterface	Yes	Yes

WMI Configurations for Windows 2008 and 2008R2

To configure WMI on your device so that FortiSIEM can discover and monitor it, you must create a user who has access to WMI objects on the device. There are two ways to do this:

- Creating a Generic User Who Does Not Belong to the Local Administrator Group
- Creating a User Who Belongs to the Domain Administrator Group
- Differences Between Administrator and Non-Administrator Account

Creating a Generic User Who Does Not Belong to the Local Administrator Group

Log in to the machine you want to monitor with an administrator account.

Step 1. Enable Remote WMI Requests by Adding a Monitoring Account to the Distributed COM Users Group and the Performance Monitor Users Group

1. Go to **Start** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Local Users and Groups**.
2. Right-click **Users** and select **New User**.
3. Create a user.
4. Select this user and right-click to select **Properties** > **Member of** tab.
5. Select **Distributed COM Users** and click **Add**.
6. Click **OK** to save.
   This is the account you must use to set up the Performance Monitor Users group permissions.
7. Repeat steps 4 through 6 for the Performance Monitor Users group.

Step 2. Enable DCOM Permissions for the Monitoring Account

1. Go to **Start** > **Control Panel** > **Administrative Tools** > **Component Services**.
2. Right-click **My Computer**, and then **Properties**.

3. Select the **COM Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
5. Click **OK**.
6. Under **Access Permissions**, click **Edit Default**.
7. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have **Local Access** and **Remote Access** set to **Allowed**.
8. Click **OK**.
9. Under **Launch and Activation Permissions**, click **Edit Limits**.
10. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. Click **OK**.
12. Under **Launch and Activation Permissions**, click **Edit Defaults**.
13. Make sure that the **Distributed COM Users** group and the **Performance Monitor Users** group have the permissions **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

See the sections on **Enabling WMI Privileges** and **Allowing WMI Access through the Windows Firewall** in the **Domain Admin User** set up instructions for the remaining steps to configure WMI.

Configuring Log Monitoring for Non-Administrative User

To configure the non-administrative user to monitor windows event logs, follow the steps below:

1. Go to **Start** > **Control Panel** > **Administrative Tools** > **Active Directory Users and Computers** (**Computer Management** > **Local Users and Groups** for servers that are not a domain controller).
2. Right-click the non-admin user and select **Properties.**
3. Select the **Member of** tab.
4. Select the group **Event Log Reader** and click **Add.**
5. Click **Apply**.
6. Click **OK** to complete the configuration.

The following groups should be applied to the user:

- **Distributed COM Users**
- **Domain Users**
- **Event Log Reader**

Creating a User Who Belongs to the Domain Administrator Group

Log in to the Domain Controller with an administrator account.

Step 1. Enable remote WMI requests by Adding a Monitoring Account to the Domain Administrators Group

1. Go to **Start** > **Control Pane** > **Administrative Tools** > **Active Directory Users and Computers** > **Users**.
2. Right-click **Users** and select **Add User**.
3. Create a user for the @accelops.com domain.
   For example, **YJTEST@accelops.com**.
4. Go to **Groups**, right-click **Administrators**, and then click **Add to Group**.

5. In the **Domain Admins Properties** dialog, select the **Members** tab, and then click **Add**.
6. For **Enter the object names to select**, enter the user you created in step 3.
7. Click **OK** to close the Domain Admins Properties dialog.
8. Click **OK**.

Step 2. Enable the Monitoring Account to Access the Monitored Device

Log in to the machine you want to monitor with an administrator account.

Enable DCOM Permissions for the Monitoring Account

1. Go to **Start > Control Panel > Administrative Tools > Component Services**.
2. Right-click **My Computer**, and then select **Properties**.
3. Select the **Com Security** tab, and then under **Access Permissions**, click **Edit Limits**.
4. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
5. Click **OK**.
6. In the **Com Security** tab, under **Access Permissions**, click **Edit Defaults**.
7. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for both **Local Access** and **Remote Access**.
8. Click **OK**.
9. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.
10. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.
11. In the **Com Security** tab, under **Launch and Activation Permissions**, click **Edit Defaults**.
12. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation**.

Enable Account Privileges in WMI

The monitoring account you created must have access to the namespace and sub-namespaces of the monitored device.

1. Go to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**.
2. Select **WMI Control**, and then right-click and select **Properties**.
3. Select the **Security** tab.
4. Expand the **Root** directory and select **CIMV2.**
5. Click **Security**.
6. Find the user you created for the monitoring account, and make sure that user has the permission **Allow** for **Enable Account** and **Remote Enable**.
7. Click **Advanced.**
8. Select the user you created for the monitoring account, and then click **Edit.**
9. In the **Apply onto** menu, select **This namespace and subnamespaces**.
10. Click **OK** to close the Permission Entry for CIMV2 dialog.
11. Click **OK** to close the Advanced Security Settings for CIMV2 dialog.
12. In the left-hand navigation, under **Services and Applications**, select **Services.**
13. Select **Windows Management Instrumentation**, and then click **Restart.**

Allow WMI to Connect Through the Windows Firewall (Windows 2003)

1. In the **Start** menu, select **Run**.
2. Run `gpedit.msc`.
3. Go to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
4. Select **Domain Profile** or **Standard Profile** depending on whether the device you want to monitor is in the domain or not.
5. Select **Windows Firewall: Allow remote administration exception**.
6. Run `cmd.exe` and enter these commands:

```
netsh firewall add portopening protocol=tcp port=135 name=DCOM_TCP135"netsh firewall add
allowedprogram program=%windir%\system32\wbem\unsecapp.exe name=UNSECAPP
```

7. Restart the server.

Allow WMI through Windows Firewall (Windows Server 2008, 2012)

1. Go to **Control Panel > Windows Firewall**.
2. In the left-hand navigation, click **Allow a program or feature through Windows Firewall**.
3. Select **Windows Management Instrumentation**, and the click **OK**.You can configure FortiSIEM to communicate with your device. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Differences Between Administrator and Non-Administrator Account

Windows allows certain WMI classes to be pulled only via Administrator account. The following table shows this clearly.

WMI Class	Administrator	Non-Administrator
Win32_BIOS	Yes	No
Win32_ComputerSystem	Yes	Yes
Win32_LogicalDisk	Yes	No
Win32_NetworkAdapter	Yes	Yes
Win32_NetworkAdapterConfiguration	Yes	Yes
Win32_NTLogEvent	Yes	Yes
Win32_OperatingSystem	Yes	Yes
Win32_Process	Yes	Yes
Win32_Processor	Yes	Yes
Win32_Product	Yes	Yes
Win32_QuickFixEngineering	Yes	No

WMI Class	Administrator	Non-Administrator
Win32_Service	Yes	No
Win32_UserAccount	Yes	No
win32_Volume	Yes	Yes
Win32_PerfFormattedData_DHCPServer_DHCPServer	Yes	Yes
Win32_PerfFormattedData_DNS_DNS	Yes	Yes
Win32_PerfFormattedData_W3SVC_WebService	Yes	Yes
Win32_PerfRawData_DirectoryServices_DirectoryServices	Yes	Yes
Win32_PerfRawData_NTDS_NTDS	Yes	Yes
Win32_PerfRawData_PerfDisk_LogicalDisk	Yes	Yes
Win32_PerfRawData_PerfDisk_PhysicalDisk	Yes	Yes
Win32_PerfRawData_PerfOS_Memory	Yes	Yes
Win32_PerfRawData_PerfOS_PagingFile	Yes	Yes
Win32_PerfRawData_PerfOS_Processor	Yes	Yes
Win32_PerfRawData_PerfProc_Process	Yes	Yes
Win32_PerfRawData_Tcpip_NetworkInterface	Yes	Yes

Windows Agent Configurations

For information on configuring Windows Agent, see Windows Agent Installation Guide.

Syslog Configurations

See the Windows Agent Installation Guide for information on configuring the sending of syslog from your device to FortiSIEM.

Sample Windows Server Syslog

```
<108>2014 Dec 17 15:05:47 CorreLog_Win_Agent 1NDCITVWCVLT05.tsi.lan Login Monitor: Local
Console User Login: User Name: weighalll-admin
```

Configuring the Security Audit Logging Policy

Because Windows generates a lot of security logs, you should specify the categories of events that you want logged and available for monitoring by FortiSIEM.

1. Log in the machine where you want to configure the policy as an administrator.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand **Local Policies** and select **Audit Policy**.
   You will see the current security audit settings.
4. Select a policy and edit the **Local Security Settings** for the events you want audited. Recommended settings are:

Policy	Description	Settings
Audit account logon events and Audit logon events	For auditing logon activity	Select **Success** and **Failure**
Audit object access events	For auditing access to files and folders. There is an additional configuration requirement for specifying which files and folders, users and user actions will be audited. See the next section, **Configuring the File Auditing Policy**.	Select **Success** and **Failure**
Audit system events	Includes system up/down messages	

Configuring the File Auditing Policy

When you enable the policy to audit object access events, you also must specify which files, folders, and user actions will be logged. You should be very specific with these settings, and set their scope to be as narrow as possible to avoid excessive logging. For this reason you should also specify system-level folders for auditing.

1. Log in the machine where you want to set the policy with administrator privileges.
   On a domain computer, a Domain administrator account is needed
2. Open Windows Explorer, select the file you want to set the auditing policy for, right-click on it, and select **Properties**.
3. In the **Security** tab, click **Advanced**.
4. Select the **Auditing** tab, and then click **Add**.
   This button is labeled **Edit** in Windows 2008.
5. In the **Select User or Group** dialog, click **Advanced**, and then find and select the users whose access to this file you want to monitor.
6. Click **OK** when you are done adding users.
7. In the **Permissions** tab, set the permissions for each user you added.

The configuration is now complete. Windows will generate audit events when the users you specified take the actions specified on the files or folders for which you set the audit policies.

Disabling Audit Token Right Adjusted Success Events

As per Microsoft, it is recommended to Disable "Success" auditing for "Audit Token Right Adjusted".

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4703#security-monitoring-recommendations.

By enabling "Success Auditing" for Audit Token Right Adjusted (Detailed Tracking), 800+ (4703) events can be generated in a second, resulting in this high volume event impacting system performance.

Complete these steps to disable "Success" for "Audit Token Right Adjusted".

1. Log in, with administrator privileges, to the machine where you want to set the policy.
   On a domain computer, you must have a Domain administrator account.
2. Go to **Programs > Administrative Tools > Local Security Policy**.
3. Expand to **Security Settings > Advanced Audit Policy Configuration > System Audit Policies - Local Group Policy Object > Detailed Tracking**.
4. Go to the **Detailed Tracking** subcategory, and select **Audit Token Right Adjusted**.
5. Double click **Audit Token Right Adjusted**, select the **Configure the following audit events:** checkbox.

6. Uncheck the **Success** checkbox if needed to disable.
7. Click **Apply**.

Configuring Print Log

FortiSIEM supports pull Windows print log from Windows agent. To configure, take the following steps.

- Enabling Logging Print Log after WMI Configuration
- Setup in FortiSIEM

Enabling Logging Print Log after WMI Configuration

After WMI Configuration is completed, enable logging print log by taking the following steps.

1. Open the **Event Viewer** window and navigate to **Applications and Services Logs > Microsoft > Windows > PrintService.**
2. Click **Operational**.
3. Right click, and select **Properties**.
4. Add a checkmark to the **Enable logging** checkbox.
5. Click **Apply**.
6. Click **OK**.

   All print activities will be logged by Event Viewer through WMI. Event logs can be viewed under **Applications and Services Logs -> Microsoft -> Windows -> PrintService -> Operational**.

Setup in FortiSIEM

Take the following steps to access print logs in FortiSIEM.

1. Log on to your Windows Server and navigate to **Event viewer > App and Service logs > Microsoft > windows > printservice > properties**.
2. Copy the full name from log properties.
3. Log onto FortiSIEM in super global.
4. Navigate to **ADMIN > Setup > Windows Agent**.
5. Under **Windows Agent Monitor Templates**, click **New** to create a Monitor Template.
6. In the **Name** field, enter a name for the template.
7. Click the **Event** tab.
8. In the Event Log row, click on **New**.
9. In the **Type** drop-down list, select **Other**.
10. In the **Event Name** field, enter/paste the full name from step 2.
11. Click **< Save**.
12. Click **Save**.
13. Under **Host to Template Associations**, create a host to template association by clicking **New**.
14. In the **Name** field, enter a name.
15. Choose an organization.
16. Select the monitor template you created through steps 5-12.
17. Select a collector.

18. Click **Save**.
19. Click **Apply**.

    FortiSIEM now automatically parses events received via WMI or FortiSIEM Windows Agent.

Setting Access Credentials

- SNMP, Telnet and SSH Access Credentials for All Devices
- LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices
- LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices
- WMI Access Credentials for All Devices

SNMP, Telnet and SSH Access Credentials for All Devices

See Access Credentials.

LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	Microsoft Windows Server *
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	OpenLDAP
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	Specify the root of the LDAP tree as the Base DN. For example: **dc=companyABC,dc=com**
Password Config	See Password Configuration
User Name	For user discoveries from an OpenLDAP directory, specify the full DN as the user name. For example: uid=jdoe,ou=hr,ou=unit,dc=companyABC,dc=com
Password	Password of the user able to access this system

LDAP, LDAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	Microsoft Windows Server *
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	Microsoft Active Directory
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	Specify the root of the LDAP tree as the Base DN. For example: **dc=companyABC,dc=com**
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	For Microsoft Active Directory, the user name can be just the login name.
Password	Password of the user able to access this system

WMI Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	Microsoft Windows Server *
Access Protocol	WMI
Pull Interval	1 minute
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

QNAP Turbo NAS

- Configuration

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Setting	Value
Name	<set name>
Device Type	QNAP Turbo NAS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to QNAP Turbo NAS.
5. To see the jobs associated with QNAP, select **ADMIN > Setup > Pull Events.**
6. To see the received events select **ANALYTICS**, then enter "QNAP" in the search box.

Sun Solaris Server

- What is Discovered and Monitored
- Event Types
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
SNMP	Host name, generic hardware (cpu, memory, network interface, disk), software (operating system version, installed software, running processes, open TCP/UDP ports)	Uptime, CPU/Memory/Network Interface/Disk space utilization, Network Interface Errors, Running Process Count, Installed Software change, Running process CPU/memory utilization, Running process start/stop, TCP/UDP port up/down	Performance Monitoring
SSH	Hardware **(cpu details, memory**)	**Memory paging rate, Disk I/O utilization**	Performance Monitoring
Syslog	Vendor, Model	General logs including Authentication Success/Failure, Privileged logons, User/Group Modification	Security Monitoring and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "solaris" to see the event types associated with this device.

Configuration

- SNMP v1 and v2c
- SSH

SNMP v1 and v2c

1. Check if the netsnmp package installed. Solaris has built-in snmp packages. If the netsnmp is not installed, use `pkgadd cmd` to install it.
2. Start snmnp with the default configuration.

SSH

1. Make sure that the `vmstat` and `iostat` commands are available. If not, install these libraries.
2. Create a user account that can issue `vmstat` and `iostat` commands. FortiSIEM will use that user account to log in to the server.

Settings for Access Credentials

- SNMP, Telnet, and SSH Access Credentials for All Devices
- LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices
- LDAP, DPAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

SNMP, Telnet, and SSH Access Credentials for All Devices

See Access Credentials.

LDAP, LDAPS, LDAP Start TLS / OpenLDAP Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	Sun Solaris
Access Protocol	LDAP / LDAPS / LDAP Start TLS
Used For	OpenLDAP
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

LDAP, DPAPS, LDAP Start TLS / Microsoft Active Directory Access Credentials for All Devices

Settings	Value
Name	<set name>
Device Type	Sun Solaris
Access Protocol	LDAP / LDAPS / LDAP Start TLS

Settings	Value
Used For	Microsoft Active Directory
Server Port	389 for LDAP, LDAP Start TLS; 636 for LDAPS
Base DN	The Distinguished Name (DN) of the starting point for directory server searches
NetBIOS/Domain	The domain name or NetBIOS name attribute
Password Config	See Password Configuration
User Name	Name of the user able to access this system
Password	Password of the user able to access this system

Storage

FortiSIEM supports these storage devices for discovery and monitoring.

- Brocade SAN Switch
- Dell Compellent Storage
- Dell EqualLogic Storage
- EMC Clarion Storage
- EMC Isilon Storage
- EMC VNX Storage
- NetApp Data ONTAP
- NetApp Filer Storage
- Nimble Storage
- Nutanix Storage

Brocade SAN Switch

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		**Hardware Status**: Fan, Power Supply, Temperature (FortiSIEM Event Type: PH_DEV_MON_HW_STATUS)	Availability Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "brocade" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Brocade San Switch
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Dell Compellent Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		**Hardware component health**: Power, Temperature, Fan	Availability Monitoring
SNMP		Volume Utilization	Performance Monitoring

Event Types

- Ping Monitoring: PH_DEV_MON_PING_STAT
- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL
- Hardware Status: PH_DEV_MON_HW_STATUS
- Disk Utilization: PH_DEV_MON_DISK_UTIL

Rules

- Availability
- Performance (Fixed Threshold)

Availability

- Storage Hardware Warning
- Storage Hardware Critical

Performance (Fixed Threshold)

- NFS Disk space Warning
- NFS Disk Space Critical

Reports

- Dell Compellent Hardware Status
- Top Dell Compellent Devices By Disk Space Util
- Top Dell Compellent Devices By Disk Space Util (Detailed)
- Top Dell Compellent modules by fan speed
- Top Dell Compellent modules by temperature
- Top Dell Compellent modules by voltage

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell Compellent Storage
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Dell EqualLogic Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		**Hardware component health**: Component name (Disk, Power supply, Temperature, Fan, RAID health), Component status, Host spare ready disk count **Overall Disk health metrics:** Total disk count, Active disk count, Failed disk count, Spare disk count	Availability Monitoring
SNMP		**Connection metrics**: Connection Count, Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) **Disk performance metrics:** Disk Name, Disk I/O Utilization, Disk I/O Queue, Read volume (KBps), Write volume (KBps) **Group level performance metrics:** Total storage, Used storage, Reserved storage, Reserved used storage, Total volumes, Used volumes, Online volumes, Total snapshot, Used snapshot, Online snapshot	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "equallogic" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "equallogic" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports**, search for "equallogic" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Dell EqualLogic
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

EMC Clariion Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
NaviSecCLI	Host name, Operating system version, Hardware model, Serial number, Network interfaces* Installed Software, Storage Controller Ports **Hardware components**: Enclosures, Fan, Power Supply, Link Control Card, CPU, Disk **RAID Groups and the assigned disk** **LUNs and LUN -> RAID Group mappings** **Storage Groups and memberships** (Host, Port, LUN).	**Processor utilization**: SP Name, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) **Port I/O**: Port name, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) **RAID Group I/O:** RAID Group id, RAID type, Total disk, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) **LUN I/O**: LUN name, LUN id, Total disk, Used disk, Free disk, Disk util, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) **Host HBA Connectivity:** Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name, Storage Group, LUN Names, Login Status, Registration Status **Host HBA Unregistered Host**: Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name **Hardware component health**: Component name (Disk, Power supply, LCC, Fan, Link, Port), Component status, Host spare ready disk count **Overall Disk health:** Total disk count, Total disk size (MB), Active disk count, Failed disk count, Spare disk count	Availability and Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "clariion" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Installing the NaviSecCLI Library in FortiSIEM

Changing NaviSecCLI Credentials

If you change the NaviSecCLI credentials on your EMC Clariion device, the certificates may also be changed and naviseccli may prompt you to accept new certificates. This should only happen the first time after a certificate change, however, FortiSIEM discovery and performance monitoring will fail. You must run NaviSecCLI manually on each Supervisor and Worker in your deployment and accept the certificate, and then rediscover your EMC Clariion device for performance monitoring to resume.

Configuration of your EMC Clariion storage device involves installing EMC's NaviSecCLI library in your FortiSIEM virtual appliance, and then setting the access credentials that the appliance will use to communicate with your device.

1. Log in to your FortiSIEM virtual appliance as `root`.
2. Copy the file `NaviCLI-Linux-64-x86-versionxyz.rpm` to the FortiSIEM directory.
3. Run `rpm --Uvh NaviCLI-Linux-64-x86-versionxyz.rpm` to install the rpm package.

```
[root@Rob-SP-94 tmp]# rpm -Uvh NaviCLI-Linux-64-x86-en_US-7.30.15.0.44-1.x86_64.rpm
Preparing... ########################################### [100%]
1:NaviCLI-Linux-64-x86-en########################################### [100%]
Please enter the verifying level(low|medium|l|m) to set?
m
Setting medium verifying level
[root@Rob-SP-94 opt]# ls -la
total 40
drwxr-xr-x 8 root root 4096 Aug 22 16:06 .
drwxr-xr-x 29 root root 4096 Aug 16 16:46 ..
drwxr-xr-x 11 admin admin 4096 Jul 23 18:56 glassfish
lrwxrwxrwx 1 root root 16 Aug 16 16:46 Java -> /opt/jdk1.6.0_32
drwxr-xr-x 8 root root 4096 Jun 2 16:35 jdk1.6.0_32
drwxr-xr-x 5 root root 4096 Aug 22 16:06 Navisphere <----Note this directory was
created***
drwxrwxr-x 14 admin admin 4096 Jul 24 11:22 phoenix
drwxrwxr-x 3 root root 4096 Jun 2 16:36 rpm
drwxr-xr-x 8 root root 4096 Jun 18 2010 vmware
[root@Rob-SP-94 opt]#
```

4. Change the user role to the admin `su - admin` and make sure that the user can run the command `naviseccli -h -User <user> -Password <pwd> -Scope global getall -sp` from the directory `/opt/phoenix/bin.`

```
[root@Rob-SP-94 Navisphere]# cd bin
[root@Rob-SP-94 bin]# su - admin
[admin@Rob-SP-94 ~]$ naviseccli
Not enough arguments
Usage:
[-User <username>] [-Password <password>]
[-Scope <0 - global; 1 - local; 2 - LDAP>]
[-Address <IPAddress | NetworkName> | -h <IPAddress | NetworkName>]
[-Port <portnumber>] [-Timeout <timeout> | -t <timeout>]
[-AddUserSecurity | -RemoveUserSecurity | -DeleteSecurityEntry]
[-Parse | -p] [-NoPoll | -np] [-cmdtime]
[-Xml] [-f <filename>] [-Help] CMD <Optional Arguments>[security -certificate]
[admin@Rob-SP-94 ~]$ pwd
/opt/phoenix/bin
```

5. Make sure that the Navisphere Analyzer module is on.
   If the module is off, performance metrics will not be available and discovery will fail. This log shows an example of the module being turned off.

```
[admin@accelops ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100
getall -sp
Server IP Address:       192.168.1.100
Agent Rev:           7.32.26 (0.95)
SP Information
--------------
Storage Processor:                  SP A
Storage Processor Network Name:     A-IMAGE
Storage Processor IP Address:       192.168.1.100
Storage Processor Subnet Mask:      255.255.255.0
Storage Processor Gateway Address:  192.168.1.254
Storage Processor IPv6 Mode:               Not Supported
Management Port Settings:
Link Status:                        Link-Up
Current Speed:                      1000Mbps/full duplex
Requested Speed:                    Auto
Auto-Negotiate:                     YES
Capable Speeds:                     1000Mbps half/full duplex
                                    10Mbps half/full duplex
                                    100Mbps half/full duplex
                                    Auto
System Fault LED:              OFF
Statistics Logging:            OFF    <----- Note: performance statistics are not being
collected
                                      <------ so AccelOp can not pull stats and
discovery will fail.
                                      <------ See how to turn ON Statistics Logging
below.
SP Read Cache State            Enabled
SP Write Cache State           Enabled
....
```

6. If the Navisphere Analyzer module is off, turn it on with the `setstats -on` command.

```
[admin@accelops ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100
setstats -on
[admin@accelops ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100
getall -sp
```

```
Server IP Address:       192.168.1.100
Agent Rev:           7.32.26 (0.95)

SP Information
--------------
Storage Processor:                  SP A
Storage Processor Network Name:     A-IMAGE
Storage Processor IP Address:       192.168.1.100
Storage Processor Subnet Mask:      255.255.255.0
Storage Processor Gateway Address:  192.168.1.254
Storage Processor IPv6 Mode:               Not Supported
Management Port Settings:
Link Status:                        Link-Up
Current Speed:                      1000Mbps/full duplex
Requested Speed:                    Auto
Auto-Negotiate:                     YES
Capable Speeds:                     1000Mbps half/full duplex
                                    10Mbps half/full duplex
                                    100Mbps half/full duplex
                                    Auto
System Fault LED:              OFF
Statistics Logging:            ON   <---NOTE that statistics Logging is now ON.
SP Read Cache State            Enabled
SP Write Cache State           Enabled
Max Requests:                  N/A
Average Requests:              N/A
Hard errors:                   N/A
Total Reads:                   1012
Total Writes:                  8871
Prct Busy:                     6.98
Prct Idle:                     93.0
System Date:                   10/04/2013
Day of the week:               Friday
System Time:                   11:23:48
Read_requests:                 1012
Write_requests:                8871
Blocks_read:                   26259
Blocks_written:                235896
Sum_queue_lengths_by_arrivals: 27398
Arrivals_to_non_zero_queue:    3649
....
```

7. Once this command runs successfully, you are ready to set the access credentials for your device in FortiSIEM and initiate the discovery process.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your EMC Clariion storage device over NaviSecCLI.

Setting	Value
Name	<set name>
Device Type	EMC Clariion
Access Protocol	Navisec CLI
Use LDAP	Select to use LDAP to access directory services
User Name	The user you configured to access NaviSecCLI
Password	The password associated with the user

EMC Isilon Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		**Hardware component health**: Component name (Disk, Power supply, Temperature, Fan), Component status (AO event type: PH_DEV_MON_HW_STATUS) **Environmental:** Temperature (AO event type: PH_DEV_MON_HW_TEMP), Voltage readings (AO event type: PH_DEV_MON_HW_VOLTAGE) **Cluster membership change**: (AO event type: PH_DEV_MON_ISILON_CLUSTER_MEMBERSHIP_CHANGE)	Availability Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "isilon" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "isilon" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports** , search for "isilon" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

EMC VNX Storage Configuration

- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Like EMC Clarion, FortiSIEM uses Navisec CLI to discover the device and to collect performance metrics. The only difference is that a slightly different command and XML formatted output is used.

Protocol	Information Discovered	Metrics collected	Used for
Navisec CLI	Host name, Operating system version, Hardware model, Serial number, Network interfaces* Installed Software, Storage Controller Ports **Hardware components**: Enclosures, Fan, Power Supply, Link Control Card, CPU, Disk **Storage Pools, RAID Groups and the assigned disks** **LUNs and LUN -> Storage Pool and RAID Group mappings** **Storage Groups and memberships** (Host, Port, LUN)	**Processor utilization**: SP Name, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) **Storage Pool I/O:** RAID Group id, RAID type, Total disk, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps)	Availability and Performance Monitoring
		LUN I/O: LUN name, LUN id, Total disk, Used disk, Free disk, Disk util, Read request rate (IOPS), Write request rate (IOPS), Read volume (KBps), Write volume (KBps), Read/Write request rate (IOPS), Read/Write volume (KBps) **Host HBA Connectivity:** Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name, Storage Group, LUN Names, Login Status, Registration Status	

Protocol	Information Discovered	Metrics collected	Used for
		Host HBA Unregistered Host: Source IP, Source Name, Source WWN, Dest IP, Destination Name, SP Port Name **Hardware component health**: Component name (Disk, Power supply, LCC, Fan, Link, Port), Component status, Host spare ready disk count **Overall Disk health:** Total disk count, Total disk size (MB), Active disk count, Failed disk count, Spare disk count	

Configuration

- Installing the NaviSecCLI Library in FortiSIEM
- Setting the IP Address for Credential Mapping

Installing the NaviSecCLI Library in FortiSIEM

Changing NaviSecCLI Credentials

If you change the NaviSecCLI credentials on your EMC Clarion device, the certificates may also be changed and naviseccli may prompt you to accept new certificates. This should only happen the first time after a certificate change, however, FortiSIEM discovery and performance monitoring will fail. You must run NaviSecCLI manually on each Supervisor and Worker in your deployment and accept the certificate, and then rediscover your EMC Clarion device for performance monitoring to resume.

Configuration of your EMC Clarion storage device involves installing EMC's NaviSecCLI library in your FortiSIEM virtual appliance, and then setting the access credentials that the appliance will use to communicate with your device.

1. Log in to your FortiSIEM virtual appliance as `root`.
2. Copy the file `NaviCLI-Linux-64-x86-versionxyz.rpm` to the FortiSIEM directory.
3. Run `rpm --Uvh NaviCLI-Linux-64-x86-versionxyz.rpm` to install the rpm package.

```
[root@Rob-SP-94 tmp]# rpm -Uvh NaviCLI-Linux-64-x86-en_US-7.30.15.0.44-1.x86_64.rpm
Preparing... ########################################### [100%]
1:NaviCLI-Linux-64-x86-en########################################### [100%]
Please enter the verifying level(low|medium|l|m) to set?
m
Setting medium verifying level
[root@Rob-SP-94 opt]# ls -la
total 40
drwxr-xr-x 8 root root 4096 Aug 22 16:06 .
drwxr-xr-x 29 root root 4096 Aug 16 16:46 ..
drwxr-xr-x 11 admin admin 4096 Jul 23 18:56 glassfish
lrwxrwxrwx 1 root root 16 Aug 16 16:46 Java -> /opt/jdk1.6.0_32
drwxr-xr-x 8 root root 4096 Jun 2 16:35 jdk1.6.0_32
drwxr-xr-x 5 root root 4096 Aug 22 16:06 Navisphere <----Note this directory was
created***
drwxrwxr-x 14 admin admin 4096 Jul 24 11:22 phoenix
```

```
drwxrwxr-x 3 root root 4096 Jun 2 16:36 rpm
drwxr-xr-x 8 root root 4096 Jun 18 2010 vmware
[root@Rob-SP-94 opt]#
```

4. Change the user role to the admin `su - admin` and make sure that the user can run the command `naviseccli -h -User <user> -Password <pwd> -Scope global getall -sp` from the directory `/opt/phoenix/bin.`

```
[root@Rob-SP-94 Navisphere]# cd bin
[root@Rob-SP-94 bin]# su - admin
[admin@Rob-SP-94 ~]$ naviseccli
Not enough arguments
Usage:
[-User <username>] [-Password <password>]
[-Scope <0 - global; 1 - local; 2 - LDAP>]
[-Address <IPAddress | NetworkName> | -h <IPAddress | NetworkName>]
[-Port <portnumber>] [-Timeout <timeout> | -t <timeout>]
[-AddUserSecurity | -RemoveUserSecurity | -DeleteSecurityEntry]
[-Parse | -p] [-NoPoll | -np] [-cmdtime]
[-Xml] [-f <filename>] [-Help] CMD <Optional Arguments>[security -certificate]
[admin@Rob-SP-94 ~]$ pwd
/opt/phoenix/bin
```

5. Make sure that the Navisphere Analyzer module is on.
If the module is off, performance metrics will not be available and discovery will fail. This log shows an example of the module being turned off.

```
[admin@accelops ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100
getall -sp
Server IP Address:       192.168.1.100
Agent Rev:           7.32.26 (0.95)
SP Information
--------------
Storage Processor:                  SP A
Storage Processor Network Name:     A-IMAGE
Storage Processor IP Address:       192.168.1.100
Storage Processor Subnet Mask:      255.255.255.0
Storage Processor Gateway Address:  192.168.1.254
Storage Processor IPv6 Mode:               Not Supported
Management Port Settings:
Link Status:                        Link-Up
Current Speed:                      1000Mbps/full duplex
Requested Speed:                    Auto
Auto-Negotiate:                     YES
Capable Speeds:                     1000Mbps half/full duplex
                                    10Mbps half/full duplex
                                    100Mbps half/full duplex
                                    Auto
System Fault LED:              OFF
Statistics Logging:            OFF    <----- Note: performance statistics are not being
collected
                                      <------ so AccelOp can not pull stats and
discovery will fail.
                                      <------ See how to turn ON Statistics Logging
below.
SP Read Cache State            Enabled
SP Write Cache State           Enabled
....
```

6. If the Navisphere Analyzer module is off, turn it on with the `setstats -on` command.

```
[admin@accelops ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100
setstats -on
[admin@accelops ~]$ naviseccli -user admin -password admin*1 -scope 0 -h 192.168.1.100
getall -sp

Server IP Address:       192.168.1.100
Agent Rev:           7.32.26 (0.95)

SP Information
--------------
Storage Processor:                   SP A
Storage Processor Network Name:      A-IMAGE
Storage Processor IP Address:        192.168.1.100
Storage Processor Subnet Mask:       255.255.255.0
Storage Processor Gateway Address:   192.168.1.254
Storage Processor IPv6 Mode:                Not Supported
Management Port Settings:
Link Status:                         Link-Up
Current Speed:                       1000Mbps/full duplex
Requested Speed:                     Auto
Auto-Negotiate:                      YES
Capable Speeds:                      1000Mbps half/full duplex
                                     10Mbps half/full duplex
                                     100Mbps half/full duplex
                                     Auto
System Fault LED:               OFF
Statistics Logging:             ON   <---NOTE that statistics Logging is now ON.
SP Read Cache State             Enabled
SP Write Cache State            Enabled
Max Requests:                   N/A
Average Requests:               N/A
Hard errors:                    N/A
Total Reads:                    1012
Total Writes:                   8871
Prct Busy:                      6.98
Prct Idle:                      93.0
System Date:                    10/04/2013
Day of the week:                Friday
System Time:                    11:23:48
Read_requests:                  1012
Write_requests:                 8871
Blocks_read:                    26259
Blocks_written:                 235896
Sum_queue_lengths_by_arrivals: 27398
Arrivals_to_non_zero_queue:     3649
....
```

7. Once this command runs successfully, you are ready to set the access credentials for your device in FortiSIEM and initiate the discovery process.

Setting the IP Address for Credential Mapping

Enter the **Storage Processor** IP address when you associate your device's access credentials to an IP address during the credential set up process. Do not enter any other IP address, such as the **Control Station** IP.

Settings for Access Credentials

Use these **Access Method Definition** settings to allow FortiSIEM to access your EMC VNX storage device over NaviSecCLI.

Setting	Value
Name	<set name>
Device Type	EMC VNX
Access Protocol	Navisec CLI
Use LDAP	Select to use LDAP to access directory services
User Name	The user you configured to access NaviSecCLI
Password	The password associated with the user

NetApp Data ONTAP

- Supported Version
- Configuration

Supported Version

FortiSIEM supports the latest NetApp ONTAP API version listed here.

- NetApp ONTAP API 8.2

Configuration

Setup in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	NetApp DataONTAP
Access Protocol	NetApp ONTAPI
Transport	- HTTP

Settings	Description
	- HTTPS
Pull Interval	5 minutes
User Name	User name for device access
Password	Password for device access
Description	Description about the device
Settings	Description

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping:
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to NetApp Data ONTAP.
5. To see the jobs associated with DataONTAP, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "DataONTAP" in the search box.

NetApp Filer Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Logical volumes, Physical Disks	Uptime, CPU utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Logical Disk Volume utilization	Availability and Performance Monitoring
SNMP		**Hardware component health**: Component name (Battery, Disk, Power supply, Temperature, Fan), Component status, Failed power supply count, Failed Fan Count **Overall Disk health metrics:** Total disk count, Active disk count, Failed disk count, Spare disk count, Reconstructing disk count, Scrubbing disk count, Add spare disk count	Availability Monitoring
SNMP		**NFS metrics**: Cache age, CIFS request rate (IOPS), NFS request rate (IOPS), Disk read rate (IOPS), Disk write rate (IOPS), Network Sent rate (Kbps), Network received rate (Kbps), RPC Bad calls, NFS Bad calls, CIFS Bad calls **Detailed NFS V3 metrics**: Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) **Detailed NFS V4 metrics**: Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) **Detailed CIFS metrics**: Total Read/Write rate (IOPS), Latency **Detailed ISCSI metrics:** Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps)	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
		Detailed FCP metrics: Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Read volume (KBps), Write volume (KBps) **Detailed LUN metrics:** LUN Name, Read request rate (IOPS), Write request rate (IOPS), Read/Write latency, Read volume (KBps), Write volume (KBps), Disk queue full	
ONTAP API		**Detailed Aggregate metrics:** Aggregate name, Read request rate (IOPS), Write request rate (IOPS), Transfer rate, CP Read rate **Detailed Volume metrics:** Volume Name, Disk Read request rate (IOPS), Disk Write request rate (IOPS), Disk read latency, Disk write latency, NFS Read request rate (IOPS), NFS Write request rate (IOPS), NFS Read latency, NFS Write latency, CIFS Read request rate (IOPS), CIFS Write request rate (IOPS), CIFS Read latency, CIFS Write latency, SAN Read request rate (IOPS), SAN Write request rate (IOPS), SAN Read latency, SAN Write latency **Detailed Disk performance metrics:** Disk Name, Disk Utilization, Read request rate (IOPS), Write request rate (IOPS), Read latency, Write latency, Transfer operations rate	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "netapp" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "netapp" in the main content panel **Search...** field to see the rules associated with this device.

Reports

In **RESOURCES > Reports** , search for "netapp" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP

1. Log in to your NetApp device with administrative privileges.
2. Go to **SNMP > Configure**.
3. For **SNMP Enabled**, select **Yes**.

4. Under **Communities**, create a `public` community with **Read-Only** permissions.
5. Click **Apply**.

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Nimble Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP		**Storage Disk Utilization**: Disk name, Total Disk, Used Disk, Free Disk, Disk Utilization	Availability Monitoring
SNMP		**Storage Performance metrics**: Read rate (IOPS), Sequential Read Rate (IOPS), Write rate (IOPS), Sequential Write Rate (IOPS), Read latency, Write latency, Read volume (KBps), Sequential Read volume (KBps), Sequential Write volume (KBps), Used Volume (MB), Used Snapshot (MB), Non-Sequential Cache Hit Ratio (FortiSIEM Event Type: PH_DEV_MON_NIMBLE_GLOBAL_STAT)	Performance Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "nimble" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Nimble Storage NimbleOS
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Nutanix Storage

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Operating system version, Hardware model, Serial number, Network interfaces, Physical Disks, Components	Uptime, Process count, CPU utilization, Real and virtual memory utilization, Disk utilization, Process CPU/Memory utilization, Network Interface metrics	Availability and Performance Monitoring
SNMP		**Disk Status**: Cluster, Controller VM, Disk id, Disk serial, Disk utilization, Total Disk, Used Disk, Free Disk **Disk Temp**: Disk Id, disk serial, Controller VM, temperature **Cluster Status:** Cluster, Cluster version, storage utilization, total storage, used storage, IOPS, latency **Service Status**: Cluster, Controller VM, Cluster VM Status, Zeus Status, Stargate Status	Availability Monitoring
SNMP		**Storage Pool Info**: Cluster, storage pool name, storage utilization, total storage, used storage, IOPS, latency **Container Info**: Cluster, Container name, storage utilization, total storage, used storage, IOPS, latency	Performance Monitoring

Event Types

- PH_DEV_MON_SYS_CPU_UTIL

  ```
  [PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
  [lineNumber]=1468,[cpuName]=Generic CPU,[hostName]=NTNX-14SM15290052-A-CVM,
  [hostIpAddr]=10.0.252.20,[cpuUtil]=100.000000,[sysCpuUtil]=0.000000,
  [userCpuUtil]=0.000000,[waitCpuUtil]=0.000000,[kernCpuUtil]=0.000000,
  [contextSwitchPersec]=0.000000,[cpuInterruptPersec]=0.000000,[pollIntv]=177,[cpuCore]=8,
  [loadAvg1min]=2.500000,[loadAvg5min]=2.500000,[loadAvg15min]=2.390000,[phLogDetail]=
  ```

- PH_DEV_MON_SYS_MEM_UTIL

```
 [PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9587,[memName]=Physical Memory,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.252.20,[memUtil]=93.210754,[pollIntv]=177,[phLogDetail]=
```

- PH_DEV_MON_SYS_VIRT_MEM_UTIL

```
 [PH_DEV_MON_SYS_VIRT_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9590,[memName]=Virtual memory,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.252.20,[virtMemUsedKB]=30773124,[virtMemUtil]=93.210754,
[pollIntv]=177,[phLogDetail]=
```

- PH_DEV_MON_SYS_UPTIME

```
[PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=1065,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.252.20,
[sysUpTime]=1815730,[sysUpTimePct]=100.000000,[sysDownTime]=0,[pollIntv]=56,
[phLogDetail]=
```

- PH_DEV_MON_SYS_DISK_UTIL

```
[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=9664,[diskName]=/home/nutanix/data/stargate-storage/disks/9XG6R3HG,
[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.252.20,[appTransportProto]=SNMP
(hrStorage),[diskUtil]=9.229729,[totalDiskMB]=938899,[usedDiskMB]=86658,
[freeDiskMB]=852241,[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_NET_INTF_UTIL

```
 [PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phIntfFilter.cpp,
[lineNumber]=319,[intfName]=eth0,[intfAlias]=,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.252.20,[pollIntv]=56,[recvBytes64]=0,[recvBitsPerSec]=0.000000,
[inIntfUtil]=0.000000,[sentBytes64]=0,[sentBitsPerSec]=0.000000,[outIntfUtil]=0.000000,
[recvPkts64]=0,[sentPkts64]=0,[inIntfPktErr]=0,[inIntfPktErrPct]=0.000000,
[outIntfPktErr]=0,[outIntfPktErrPct]=0.000000,[inIntfPktDiscarded]=0,
[inIntfPktDiscardedPct]=0.000000,[outIntfPktDiscarded]=0,
[outIntfPktDiscardedPct]=0.000000,[outQLen64]=0,[intfInSpeed64]=10000000000,
[intfOutSpeed64]=10000000000,[intfAdminStatus]=up,[intfOperStatus]=up,
[daysSinceLastUse]=0,[totIntfPktErr]=0,[totBitsPerSec]=0.000000,[phLogDetail]=
```

- PH_DEV_MON_PROC_RESOURCE_UTIL

```
[PH_DEV_MON_PROC_RESOURCE_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=4378,[swProcName]=python,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.23.20,[procOwner]=,[memUtil]=0.379639,[cpuUtil]=0.000000,
[appName]=python,[appGroupName]=,[pollIntv]=116,[swParam]=/home/nutanix/ncc/bin/health_
server.py --log_plugin_output=true --logtostderr=true,[phLogDetail]=
```

- PH_DEV_MON_SYS_PROC_COUNT

```
[PH_DEV_MON_SYS_PROC_COUNT]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=11378,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.252.20,
[procCount]=327,[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_DISK_STATUS

```
[PH_DEV_MON_NUTANIX_DISK_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=216,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,
[cluster]=AmanoxLab01,[diskId]=24,[ntxControllerVMId]=7,[hwDiskSerial]=9XG6V4DS,
[diskUtil]=35.704633,[totalDiskMB]=916,[freeDiskMBNonRoot]=589,[inodeUsedPct]=0.234492,
[inodeMax]=61054976,[inodeFreeNonRoot]=60911807,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_CLUSTER_STATUS

```
[PH_DEV_MON_NUTANIX_CLUSTER_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=272,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,
[cluster]=Lab01,[clusterVersion]=el6-release-danube-4.1.2-stable-
99e1e2dda7a78989136f39132e1f198989ef03a4,[clusterStatus]=started,[diskUtil]=32.000000,
[totalDiskMB]=14482532,[usedDiskMB]=4740567,[diskRWReqPerSec]=3109.000000,
[devDiskRWLatency]=0.631000,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_SERVICE_STATUS

```
[PH_DEV_MON_NUTANIX_SERVICE_STATUS]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=287,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,
[cluster]=Lab01,[ntxControllerVMId]=5,[ntxClusterVMStatus]=Up,[ntxZeusStatus]=3287,
3310, 3311, 3312, 3389, 3403,[ntxStargateStatus]=5331, 5365, 5366, 5421, 19543,
[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO

```
[PH_DEV_MON_NUTANIX_STORAGE_POOL_INFO]:[eventSeverity]=PHL_INFO,
[fileName]=devNutanix.cpp,[lineNumber]=239,[hostName]=NTNX-14SM15290052-A-CVM,
[hostIpAddr]=10.0.23.20,[cluster]=Lab01,[spoolId]=1474,[spoolName]=amanoxlab_sp,
[diskUtil]=32.733000,[totalDiskMB]=14482532,[usedDiskMB]=4740567,
[diskRWReqPerSec]=155.000000,[devDiskRWLatency]=0.631000,[phLogDetail]=
```

- PH_DEV_MON_NUTANIX_CONTAINER_INFO

```
[PH_DEV_MON_NUTANIX_CONTAINER_INFO]:[eventSeverity]=PHL_INFO,[fileName]=devNutanix.cpp,
[lineNumber]=257,[hostName]=NTNX-14SM15290052-A-CVM,[hostIpAddr]=10.0.23.20,
[cluster]=Lab01,[ntxContainerId]=1488,[ntxContainerName]=perflab_ndfs,
[diskUtil]=8.357116,[totalDiskMB]=14482532,[usedDiskMB]=1210322,
[diskRWReqPerSec]=0.000000,[devDiskRWLatency]=0.000000,[phLogDetail]=
```

Rules

Currently there are no system rules defined.

Reports

- Nutanix Cluster Disk Usage
- Nutanix Cluster Performance
- Nutanix Cluster Service Status
- Nutanix Cluster Storage Usage
- Nutanix Container Performance
- Nutanix Container Storage Usage
- Nutanix Storage Pool Performance
- Nutanix Storage Pool Usage

Configuration

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the

User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Nutanix Controller VM
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Threat Intelligence

FortiSIEM supports these threat detection devices:

- FortiAI
- FortiInsight
- LastLine
- ThreatConnect

External threat intelligence sources provide information about malware actors (Indicators of Compromise or IOCs). FortiSIEM can be configured to download this information periodically, either incrementally or full updates, according to a schedule you define. IOCs can include Malware IP, Domain, URL, and file hashes. You can write rules to look for matches in real time or reports to look for matches in historical data.

The following external threat intelligence sources are supported out of the box:

- Emerging Threat
- FortiGuard
- FortiSandbox
- Malware Domain
- SANS
- ThreatStream
- ThreatConnect
- TruSTAR
- Zeus

In general, any threat source that provides a CSV file or supports STIC/TAXII standards 1.0, 1.1, and 2.0 can be automatically supported by FortiSIEM. FortiSIEM also provides a Java-based API which can be used to support a new website.

Fortinet FortiAI

- Event Types
- Rules
- Reports
- Configuration

Event Types

In **ADMIN > Device Support > Event Types**, search for "fortiai" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "fortiai" in the main content panel **Search...** field to see related rules associated with this device.

- FortiAI: Attack Chain Blocked
- FortiAI: Attack Chain Permitted

Reports

In **RESOURCES > Reports**, search for "fortiai" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514.

FortiAI Syslog Configuration

See the current FortiAI Administration Guide for the latest configuration information under Log & Report. The instructions provided here are based off the 1.5.0 FortiAI Administration Guide.

1. From the FortiAI GUI, navigate to **Log and Report > Log Settings > Remote Log Server**.
2. Set **Send logs to FortiSIEM** to **Enable**.
3. Set **Type** to **Syslog**.
4. In the **Log Server Address** field, enter the IP address or FQDN of the FortiSIEM Collector.
5. In the Port field, enter "514".
6. Click **OK**.

Fortinet FortiInsight

FortiInsight is a unique data security and threat detection solution that delivers advanced threat hunting to help you spot, respond to, and manage risky behaviors that put your business-critical data at risk. It combines powerful and flexible Machine Learning with detailed forensics around user actions to bring focus to the facts more rapidly than other solutions.

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration in FortiInsight
- Configuration in FortiSIEM
- Sample Events

What is Discovered and Monitored

Protocol	Information collected	Used for
FortiInsight API	Policy based alerts and AI based alerts	Data security, threat protection

This feature allows FortiSIEM to get Policy-based alerts and AI-based alerts from FortiInsight.

Event Types

In **RESOURCES > Event Types**, enter "FortiInsight" in the main content panel **Search...** field to see the event types associated with this device.

Rules

No defined rules.

Reports

In **RESOURCES > Reports**, enter "FortiInsight" in the main content panel **Search...** field to see the rules associated with this device.

Configuration in FortiInsight

Get an API Key in FortiInsight

Complete these steps in the FortiInsight UI:

1. Login to FortiInsight.
2. Select **Admin > Account** from the left menu.

3. Click **New API Key** to open the New API Key dialog box.
4. Enter a descriptive **Name**.
5. Click **Save** to generate the API key. This will download a file containing the API key information (**Client ID**, **Client Secret**, and **Name**). Make a note of these values; you will need them when you configure FortiSIEM.

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential
Device Type	Fortinet FortiSIEM
Access Protocol	FortiInsight API
Pull Interval	The interval in which FortiSIEM will pull events from FortiInsight. Default is 3 minutes.
Client ID	Access key for your FortiInsight instance.
Client Secret	Secret key for your FortiInsight instance
Organization	The organization the device belongs to.
Description	Description of the device.

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your Fortinet FortiInsight credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to FortiInsight.
5. To see the jobs associated with FortiInsight, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "FortiInsight" in the search box.

Sample Events

```
[FORTIINSIGHT_POLICY_ALERT] = {"description":"","events":[{"act":"file
downloaded","app":"chrome.exe","childId":null,"d":"2019-03-
18T13:22:24.344+00:00","id":null,"m":"uqP","mn":{"dh":"tcp://server-10-230-2-
153.lhr5.r.cloudfront.net","dip":"10.1.1.76","dp":61024,"ext":".mkv","fp":"c:\\users\\Admini
strator\\documents\\secret\\prototypedemo1.mkv","fs":2307792448,"loc":
```

```
{"altCode":null,"city":"Augsburg","code":"DE","country":"Germany","latitude":"48.3718","long
itude":"10.8925"},"p":"tcp-ip-
4","sip":"78.47.38.226","sp":443,"ts":1460},"r":"c:\\users\\Administrator\\documents\\secret
\\prototypedemo1.mkv-> tcp://server-54-230-2-153.lhr5.r.cloudfront.net:443","u":"acmeltd__
engineer2"}],"extendedEvents":[{"act":"file
downloaded","app":"chrome.exe","childId":null,"d":"2019-03-
18T13:22:24.344+00:00","id":null,"latestHostname":"mimas","latestIp":"10.10.0.1","m":"uqP","
mn":{"dh":"tcp://server-54-230-2-
153.lhr5.r.cloudfront.net","dip":"10.1.1.76","dp":61024,"ext":".mkv","fp":"c:\\users\\Admini
strator\\documents\\secret\\prototypedemo1.mkv","fs":2307792448,"loc":
{"altCode":null,"city":"Augsburg","code":"DE","country":"Germany","latitude":"48.3718","long
itude":"10.8925"},"p":"tcp-ip-
4","sip":"78.47.38.226","sp":443,"ts":1460},"r":"c:\\users\\Administrator\\documents\\secret
\\prototypedemo1.mkv-> tcp://server-10-230-2-
153.lhr5.r.cloudfront.net:443","resolvedUsername":"","u":"acmeltd__
engineer2"}],"id":"AWmQ98PYg7b_-i6_5Rvg","labels":[""],"policyId":"default_
6COnUMjTCB8N","policyName":"Browser Download","regimes":
["ZoneFox"],"serverIp":"52.209.49.52","serverName":"fortisiemtest.dev.fortiinsight.cloud","s
everity":10,"status":"New","time":"2019-03-18T13:22:29.473715+00:00"}
```

Lastline

The Lastline parser collects syslog log events in CEF format.

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Syslog
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog	Device Type	Endpoint activity such as file download, email attachments, network connections.	Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "Lastline" to see the event types associated with this device.

Rules

There are no specific rules for Lastline, however rules that match the Event Type Groups associated with Lastline Events may trigger.

Reports

There are no specific Reports for Lastline, however reports that match the Event Type Groups associated with Lastline Events may return results.

Syslog

FortiSIEM processes events from this device via syslog. Configure the device to send syslog to FortiSIEM on port 514 using CEF formatting.

Sample Events

```
Aug 13 14:48:37 fortisiem CEF:0|Lastline|Enterprise|7.10|appliance-status|Appliance
Status|1|cat=Online cs1=SENSOR cs1Label=deviceType
cs2=https://example/portal#/appliances/config/status/76b80c7ac11a4d37bc6b29e66726b01d
```

```
cs2Label=deviceStatusLink deviceExternalId=76b80c7ac11a4d37bc6b29e66726b01d dvc=10.31.61.152
dvchost=example.com end=Aug 13 2018 16:48:37 CEST rt=Aug 13 2018 16:48:37 CEST start=Aug 13
2018 16:48:37 CEST
```

ThreatConnect

- What is Discovered and Monitored
- Configuring ThreatConnect
- Configuring FortiSIEM to Download IOCs from ThreatConnect
- Downloading Other IOCs

What is Discovered and Monitored

Protocol	Information Collected	Used For
ThreatConnect API	Malware Domain, IP, URL and Hash	Detect threats for Security and Compliance

Configuring ThreatConnect

Create an API Key to be used for FortiSIEM communication.

The details are here:

https://kb.threatconnect.com/customer/en/portal/articles/2188549-creating-user-accounts

1. Log in to your ThreatConnect portal as an administrative user.
2. Go to **My Profile > ORG Settings**.
3. Click **Create API User**.
   These credentials will be created:
   - **Access ID**
   - **Secret Key**
4. Note the **Organization Name.** You will need it in a later step.
5. ThreatConnect contains many threat feeds. If you want to get specific threatfeeds, then you must know the threat feeds that are available for your account. You can see these feeds by navigating to **Browse > Indicators > My ThreatConnect > Intelligent Sources**.

Configuring FortiSIEM to Download IOCs from ThreatConnect

Use the Access ID and Secret Key that were created in the previous section to enable FortiSIEM access.

FortiSIEM can provide the following IOCs from ThreatConnect:

- Malware Domain
- Malware IP
- Malware URL
- Malware Hash

Follow these steps to set up **Malware Domain** downloads from ThreatConnect.

1. Login to FortiSIEM.
2. Go to **RESOURCES > Malware Domain > ThreatConnect Malware Domain**.
3. Click **More > Update**. Select **Update via API**.

4. Enter the following fields
   a. Set **User Name** to Access ID (Step 3a above).
   b. Set **Password** to Secret Key (Step 3b above).
   c. Set **Data Format** to STIX-TAXII.
   d. For **Collection:**, you have two choices:
      - To get *all* threatfeeds - enter All:<Organization Name> (Step 4 above), or
      - To get *specific* threatfeeds, enter comma-separated values of threatfeeds (obtained from Step 6 above).
   e. Set **Data Update** = Incremental
5. Click **Save**.
6. Click **Schedule** to specify how often the threat feed will be updated.
   a. Choose **Start time**.
   b. Choose **Recurrence pattern**.
   c. Click **Save**.
7. Wait until the first scheduled download occurs. Then, navigate to **RESOURCES > Malware Domain > ThreatConnect Malware Domain.** Downloaded Malware domains will be displayed in the right-hand table. You can use this object in rules and reports to detect hits.

Downloading Other IOCs

The steps for configuring FortiSIEM to download other IOCs are identical, except for the following details:

- Malware IP—Navigate to **RESOURCES > Malware Domain > ThreatConnect Malware IP**
- Malware URL—Navigate to **RESOURCES > Malware Domain > ThreatConnect Malware URL**
- Malware Hash—Navigate to **RESOURCES > Malware Domain > ThreatConnect Malware Hash**

Virtualization

FortiSIEM supports these virtualization servers for discovery and monitoring.

- Hyper-V
- HyTrust CloudControl
- KVM
- VMware ESX

Hyper-V

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
Powershell over WMI		CPU, Memory, Network and Storage metrics both at Guest and Host level .	Performance Monitoring

Event Types

- PH_DEV_MON_HYPERV_OVERALL_HEALTH: HyperV Machine Health Summary

```
[PH_DEV_MON_HYPERV_OVERALL_HEALTH]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[vmHealthCritCount]=0,[vmHealthOkCount]=10
```

- PH_DEV_MON_HYPERV_OVERALL_SYSINFO: HyperV System Information

```
[PH_DEV_MON_HYPERV_OVERALL_SYSINFO]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[notificationCount]=10,[virtualProcessors]=52,[totalPages]=67290,
[partitionCount]=6,[logicalProcessors]=16
```

- PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC: HyperV Logical Processor Usage

```
[PH_DEV_MON_HYPERV_CPU_LOGICAL_PROC]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[idleTimePct]=47.30,[guestRunTimePct]=50.88,[hypervisorRunTimePct]=1.97,
[totalRunTimePct]=52.84,[cpuInterruptPerSec]=53390.62,[contextSwitchPerSec]=85516.44
```

- PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC: HyperV Root Virtual Processor Usage

```
[PH_DEV_MON_HYPERV_CPU_ROOT_VIRTUAL_PROC]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[phyMachIpAddr]=172.16.20.180,[phyMachName]=WIN-HH2MFBPMHMR,
[guestRunTimePct]=0.19,[hypervisorRunTimePct]=0.04,[totalRunTimePct]=0.23,
[cpuInterruptPersec]=4588.63,[interceptCost]=1458
```

- PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC: HyperV Guest Virtual Processor Usage

```
[PH_DEV_MON_HYPERV_CPU_GUEST_VIRTUAL_PROC]:[hostIpAddr]=172.16.20.185,
[hostName]=accelops-reporter-hyperv-4.3.1.1158,[vmName]=accelops-reporter-hyperv-
4.3.1.1158,[phyMachIpAddr]=172.16.20.180,[phyMachName]=WIN-HH2MFBPMHMR,
[guestRunTimePct]=1.06,[hypervisorRunTimePct]=0.70,[totalRunTimePct]=1.77,
[cpuInterruptPersec]=6474.56,[interceptCost]=1086
```

- PH_DEV_MON_HYPERV_MEM_PARTITION: HyperV Memory Partition usage

```
[PH_DEV_MON_HYPERV_MEM_PARTITION]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,
[1gGpaPages]=0,[2mGpaPages]=16385,[4kGpaPages]=9949,[depositedGpaPages]=20946
```

- PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM: HyperV per-VM Memory Partition usage

```
[PH_DEV_MON_HYPERV_MEM_PARTITION_PER_VM]:[phyMachIpAddr]=172.16.20.180,
[phyMachName]=WIN-HH2MFBPMHMR,[hostIpAddr]=172.16.20.182,[hostName]=accelops-va-hyperv-
4.3.1.1158,[vmName]=accelops-va-hyperv-4.3.1.1158,[1gGpaPages]=0,[2mGpaPages]=4096,
[4kGpaPages]=2089,[depositedGpaPages]=5044
```

- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION: HyperV Root Partition Total Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[1gGpa]=0,[2mGpa]=32613,[4kGpa]=9760,[depositedGpa]=46344
```

- PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT: HyperV Root Partition Root Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_ROOT_PARTITION_ROOT]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[1gGpa]=0,[2mGpa]=32613,[4kGpa]=9760,[depositedGpa]=46344
```

- PH_DEV_MON_HYPERV_MEM_VID_PARTITION: HyperV VID Partition Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_VID_PARTITION]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[physicalPages]=8398888,[remotePages]=0
```

- PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM: HyperV per-VM VID Partition Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_VID_PARTITION_PER_VM]:[phyMachIpAddr]=172.16.20.180,
[phyMachName]=WIN-HH2MFBPMHMR,[hostIpAddr]=172.16.20.185,[hostName]=accelops-reporter-
hyperv-4.3.1.1158,[vmName]=accelops-reporter-hyperv-4.3.1.1158,[physicalPages]=1050632,
[remotePages]=0
```

- PH_DEV_MON_HYPERV_MEM_OVERALL: HyperV Root Memory Usage

```
[PH_DEV_MON_HYPERV_MEM_OVERALL]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,
[freeMemKB]=27519348,[pageFaultsPersec]=0
```

- PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH: HyperV Virtual Switch Network Usage

```
[PH_DEV_MON_HYPERV_NET_VIRTUAL_SWITCH]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[vSwitch]=broadcom bcm5709c netxtreme ii gige [ndis vbd client] _34 -
virtual switch,[recvBitsPerSec]=719403.45,[recvPktsPerSec]=323.03,
[sentBitsPerSec]=3382443.50,[sentPktsPerSec]=283.90,[totalPktsPerSec]=323.03[PH_DEV_MON_
HYPERV_NET_VIRTUAL_SWITCH]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-HH2MFBPMHMR,
[vSwitch]=broadcom bcm5709c netxtreme ii gige [ndis vbd client] _34 - virtual switch,
[recvBitsPerSec]=719403.45,[recvPktsPerSec]=323.03,[sentBitsPerSec]=3382443.50,
[sentPktsPerSec]=283.90,[totalPktsPerSec]=323.03
```

- PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER: HyperV Virtual Switch Per Adapter Network Usage

```
[PH_DEV_MON_HYPERV_NET_VIRTUAL_ADAPTER]:[phyMachIpAddr]=172.16.20.180,[phyMachName]=WIN-
HH2MFBPMHMR,[hostIpAddr]=172.16.20.182,[hostName]=accelops-va-hyperv-4.3.1.1158,
[vmName]=accelops-va-hyperv-4.3.1.1158,[intfName]=adapter_e1eb0a1f-1b36-48fe-be79-
fde20d335364--31575d2f-5085-45d3-905f-2f3e17342a81,[recvBitsPerSec]=64970.24,
[recvPktsPerSec]=20.86,[sentBitsPerSec]=124741.68,[sentPktsPerSec]=42.61,
[totalPktsPerSec]=20.86
```

- PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE: HyperV Virtual Storage Usage

```
[PH_DEV_MON_HYPERV_STORAGE_VIRTUAL_STORAGE]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
HH2MFBPMHMR,[diskName]=e:-hyperinstance-report431-virtual hard disks-accelops-reporter-
4.3.1.1158-disk2.vhdx,[diskErrors]=2,[diskFlushes]=1267221,[diskReadKBytesPerSec]=0.00,
[diskReadReqPerSec]=0.00,[diskWriteKBytesPerSec]=0.00,[diskWriteReqPerSec]=0.00
```

- PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK: HyperV Logical Disk Usage

  ```
  [PH_DEV_MON_HYPERV_STORAGE_LOGICAL_DISK]:[hostIpAddr]=172.16.20.180,[hostName]=WIN-
  HH2MFBPMHMR,[diskName]=e:,[ioReadLatency]=0,[ioWriteLatency]=14
  ```

Rules

- HyperV Disk I/O Warning
- HyperV Disk I/O Critical
- HyperV Guest Critical
- HyperV Guest Hypervisor Run Time Percent Warning
- HyperV Logical Processor Total Run Time Percent Critical
- HyperV Logical Processor Total Run Time Percent Warning
- HyperV Page fault Critical
- HyperV Page fault Warning
- HyperV Remainining Guest Memory Warning

Reports

Look in **RESOURCES > Reports** > **Device** > **Server** > **HyperV**

- HyperV Configuration and Health
- Top HyperV Guests By Virtual Processor Run Time Pct
- Top HyperV Guests by Large Page Size Usage
- Top HyperV Guests by Remote Physical Page Usage
- Top HyperV Root Partitions By Virtual Processor Run Time Pct
- Top HyperV Root Partitions by Large Page Size Usage
- Top HyperV Servers By Logical Processor Run Time Pct
- Top HyperV Servers by Disk Activity
- Top HyperV Servers by Disk Latency
- Top HyperV Servers by Large Page Size Usage
- Top HyperV Servers by Memory Remaining for Guests
- Top HyperV Servers by Remote Physical Page Usage

Configuration

FortiSIEM needs WMI credentials to get the Hyper-V performance metrics. Configure this following the guidelines described in Microsoft Windows Server Configuration.

Settings for Access Credentials

Configure WMI on FortiSIEM.

HyTrust CloudControl

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Data Collected	Used for
Syslog (CEF format)	-	Over 70 event types	Security and Compliance

Event Types

In **RESOURCES > Event Types**, search for "HyTrust-" in the main content panel **Search...** field to see the event types associated with this device or application.

Sample Event Type:

```
<172>Mar 22 03:32:36 htcc136.test.hytrust.com local5: CEF:0|HyTrust|HyTrust
CloudControl|5.0.0.50821|ARC0031|TEMPLATE_OPERATION_ERRORED_ERR|6| rt=Mar 22 2017
03:32:36.196 UTC act=HostOperation dst=192.168.213.154 src=192.168.213.10 suser=ARC
deviceExternalId=6u1b-esxi2.test.hytrust.com deviceFacility=HostSystem msg=Template
operation VHG6.0 esxi-check-patch-version error  on host 6u1b-esxi2.test.hytrust.com
(192.168.213.154). privilege={}
```

Rules

There are no specific rules but generic rules for Security Manager and Generic Servers apply.

Reports

There are no specific reports but generic rules for Security Manager and Generic Servers apply.

Configuration

Configure HyTrust CloudControl to send syslog on port 514 to FortiSIEM.

KVM

FortiSIEM Support added: 6.3.1

FortiSIEM last modification: 6.3.1

Vendor version tested: Not Provided

Vendor: Free Software released under the General Public License (GPL).

Product Information: https://www.linux-kvm.org/page/Main_Page

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Logs

What is Discovered and Monitored

Method	Information discovered	Metrics collected	Logs collected	Used for
syslog	Host name, Reporting IP	None	Virtual Machine monitoring and changes	Security Monitoring

Event Types

- LINUX_Auditd_VIRT_MACHINE_ID
- LINUX_Auditd_VIRT_CONTROL
- LINUX_Auditd_VIRT_RESOURCE

Rules

There are no specific rules.

Reports

There are no specific reports.

Configuration

To configure, take the following steps:

1. Install auditd daemon on linux host. (i.e apt-get install auditd)
2. Edit `/etc/audit/auditd.conf` and configure as follows (take note of `log_format = ENRICHED` as this provides the real users behind the UIDs and AUIDs):

   Note: This file controls the configuration of the audit daemon.

   ```
   local_events = yes
   write_logs = yes
   log_file = /var/log/audit/audit.log
   log_group = root
   log_format = ENRICHED
   flush = INCREMENTAL_ASYNC
   freq = 50
   max_log_file = 8
   num_logs = 5
   priority_boost = 4
   disp_qos = lossy
   dispatcher = /sbin/audispd
   name_format = NONE
   ##name = mydomain
   max_log_file_action = ROTATE
   space_left = 75
   space_left_action = SYSLOG
   action_mail_acct = root
   admin_space_left = 50
   admin_space_left_action = SUSPEND
   disk_full_action = SUSPEND
   disk_error_action = SUSPEND
   use_libwrap = yes
   ##tcp_listen_port =
   tcp_listen_queue = 5
   tcp_max_per_addr = 1
   ##tcp_client_ports = 1024-65535
   tcp_client_max_idle = 0
   enable_krb5 = no
   krb5_principal = auditd
   ##krb5_key_file = /etc/audit/audit.key
   distribute_network = no
   ```

3. Configure rsyslog to send this logfile via syslog by editing `/etc/rsyslog.conf` and adding these lines:

   Note: This does not need Linux agent.

   ```
   $ModLoad imfile
   $InputFileName /var/log/audit/audit.log
   $InputFileTag tag_audit_log:
   $InputFileStateFile audit_log
   $InputFileSeverity info
   $InputFileFacility local6
   $InputRunFileMonitor
   *.* @replace.with.fortisiem.collector.IP:514
   ```

Sample Logs

Sample logs are provided here. For more information on logs, see https://libvirt.org/auditlog.html.

```
<182>Jul 26 15:20:36 fsa3000e4 tag_audit_log: type=VIRT_CONTROL msg=audit
(1627305635.364:82451): pid=25686 uid=0 auid=4294967295 ses=4294967295 msg='virt=kvm
op=start reason=booted vm="DT_FSR_Agent" uuid=104735e9-c1ea-44bc-8d99-0fe6fde58b73 vm-
pid=25722 exe="/usr/sbin/libvirtd" hostname=? addr=? terminal=? res=success'UID="root"
AUID="unset"
```

```
<182>Jul 26 15:20:36 fsa3000e4 tag_audit_log: type=VIRT_RESOURCE msg=audit
(1627305634.788:82437): pid=25686 uid=0 auid=4294967295 ses=4294967295 msg='virt=kvm
resrc=net reason=open vm="DT_FSR_Agent" uuid=104735e9-c1ea-44bc-8d99-0fe6fde58b73
net=52:54:00:e7:84:3c path="/dev/net/tun" rdev=0A:C8 exe="/usr/sbin/libvirtd" hostname=?
addr=? terminal=? res=success'UID="root" AUID="unset"
```

```
<182>Jul 26 15:20:36 fsa3000e4 tag_audit_log: type=VIRT_MACHINE_ID msg=audit
(1627305634.632:82435): pid=25686 uid=0 auid=4294967295 ses=4294967295 msg='virt=kvm vm="DT_
FSR_Agent" uuid=104735e9-c1ea-44bc-8d99-0fe6fde58b73 vm-ctx=+64055:+64055 img-
ctx=+64055:+64055 model=dac exe="/usr/sbin/libvirtd" hostname=? addr=? terminal=?
res=success'UID="root" AUID="unset"
```

VMware ESX

- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
VMWare SDK	ESX Server and the Guest hosts running on that server. ESX host clusters. Hardware (CPU, Memory, Disk, network Interface) for all guests, OS vendor and version for all guests. Virtual switch for connecting guest hosts to network interfaces.	Both ESX level and guest host level performance metrics. **Guest host level metrics** include CPU/memory/disk utilization, CPU Run/Ready/Limited percent, memory swap in/out rate, free memory state, disk read/write rate/latency, network interface utilization, errors, bytes in/out. **ESX level metrics** include physical CPU utilization, ESX kernel disk read/writre latency etc	Performance Monitoring
VMWare SDK		ESX logs include scenarios like ESX level login sucess/failure, configuration change, Guest host movement, account creation and modification	Availability, Change and Security Monitoring

Configuration

FortiSIEM discovers and monitors VMware ESX servers and guests over the the VMware SDK. Make sure that VMware Tools is installed on all the guests in your ESX deployment, and FortiSIEM will be able to obtain their IP addresses.

Settings for Access Credentials

- User with System View Credentials
- Settings for VMware ESX VMSDK Access Credentials

User with System View Credentials

Make sure to provide a user with **System View** permissions who can access the entire vCenter hierarchy when setting up the access credentials for your VMware ESX device. See the VMware documentation on how to se tup a user with

System View permissions.

Settings for VMware ESX VMSDK Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	VMware ESX Server
Access Protocol	VM SDK
User Name	A user with System View permissions
Password	The password associated with the user

VPN Gateways

FortiSIEM supports these VPN gateways for discovery and monitoring.

- Cisco VPN 3000 Gateway
- Cyxtera AppGuard
- Juniper Networks SSL VPN Gateway
- Microsoft PPTP VPN Gateway
- Pulse Secure

Cisco VPN 3000 Gateway

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco_vpn" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP

1. Log in to your device with administrative credentials.
2. Go to **Configuration > System > Management Protocols > SNMP Communities**.
3. Click **Add**.
4. For **Community String**, enter `public`.

Syslog

1. Go to **Configuration > System > Events > Syslog Servers**.
2. Click **Add**.
3. Enter the IP address of your FortiSIEM virtual appliance for Syslog Server.
4. Add a syslog server with FortiSIEM IP Address.

Sample Parsed Cisco VPN 3000 Syslog Message

```
<189>18174 01/07/1999 20:25:27.210 SEV=5 AUTH/31 RPT=14  User [ admin ] Protocol [ Telnet ]
attempted ADMIN logon. Status: <REFUSED> authentication failure
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco VPN 3K
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cyxtera AppGate Software Defined Perimeter (SDP)

- Integration Points
- Event Types
- Configuring Cyxtera AppGate Software

Integration Points

Protocol	Information Discovered	Used For
Syslog	Access Control log	Security and Compliance

Event Types

Over 70 events are parsed. See event types in **RESOURCES > Event Types** and search for "Cyxtera-AppGate-SDP" in the main content panel **Search...** field.

Configuring Cyxtera AppGate Software

Follow Cyxtera AppGate SDP documentation to send syslog to FortiSIEM.

Configuring FortiSIEM

FortiSIEM automatically recognizes Cyxtera AppGate syslog, so long as it follows the following format as shown in the sampel syslog:

```
"id":"a51e7e7d-ab5f-444c-b7f8-ca72e4bb940b","timestamp":"2018-10-
09T10:23:43.992Z","event_type":"ip_access","version":8,"distinguished_
name":"CN=0f1a40d612f741228d7cb73a4308bea8,CN=abc,OU=ACME","entitlement_token_
id":"78174080-a34","action":"allow","direction":"down","client_ip":"1.1.1.1","client_
port":1392,"packet_size":40,"protocol":"TCP","source_ip":"10.1.1.1","destination_
ip":"10.1.1.1","source_port":56100,"destination_port":59721,"connection_
type":"established","rule_name":"rule1"
```

Juniper Networks SSL VPN Gateway

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Parsed Juniper Networks SSL VPN Syslog Messages
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "junos_dynamic_vpn" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- Syslog

SNMP

1. Log into your device with administrative credentials.
2. Go to **System > Log/Monitoring > SNMP**.
3. Under **Agent Properties**, enter `public` for **Community**.

Syslog

- VPN Access Syslog
- Admin Access Syslog

VPN Access Syslog

1. Go to **System > Log/Monitoring > User Access > Settings**.
2. Under **Select Events to Log**, select **Login/logout**, **User Settings**, and **Network Connect**.
3. Under **Syslog Servers**, enter the IP address of your FortiSIEM virtual appliance, and set the **Facility** to **LOCAL0**.
4. Click **Save Changes**.

Admin Access Syslog

1. Go to **System > Log/Monitoring > Admin Access > Settings**.
2. Under **Select Events to Log**, select **Administrator changes**, **License Changes**, and **Administrator logins**.
3. Under **Syslog Servers**, enter the IP address of your FortiSIEM virtual appliance, and set the **Facility** to **LOCAL0**.
4. Click **Save Changes**.

Sample Parsed Juniper Networks SSL VPN Syslog Messages

```
<134>Juniper: 2008-10-28 04:34:53 - ive - [192.168.20.82] admin(Users)[] - Login failed
using auth server SteelBelted (Radius Server).  Reason: Failed

<134>Juniper: 2008-10-28 03:12:03 - ive - [192.168.20.82] wenyong(Users)[Users] - Login
succeeded for wenyong/Users from 192.168.20.82.

<134>Juniper: 2008-10-28 03:55:20 - ive - [192.168.20.82] wenyong(Users)[Users] - Network
Connect: Session ended for user with IP 172.16.3.240

<134>Juniper: 2008-10-28 03:05:25 - ive - [172.16.3.150] admin(Admin Users)[] - Primary
authentication successful for admin/Administrators from 172.16.3.150

<134>Juniper: 2008-10-28 05:33:02 - ive - [172.16.3.150] admin(Admin Users)[] - Primary
authentication failed for admin/Administrators from 172.16.3.150
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

Microsoft PPTP VPN Gateway

- Configuring Microsoft PPTP
- Sample Syslog Messages

Configuring Microsoft PPTP

Windows 2003 Server

1. Logon with administrative rights.
2. Configure PPTP VPN.
    a. Go to Start | All Programs | Administrative Tools | Configure Your Server Wizard, select the Remote Access/VPN Server role. The click the next button which runs the the Routing and Remote Access Wizard.
    b. On the Routing and Remote Access wizard, follow the following steps:
        i. Select "Virtual Private Network (VPN) and NAT" and click Next.
        ii. Select the network interface for use by VPN connection and click Next.
        iii. Specify the network that VPN clients should connect to in order to access resources and click Next.
        iv. Select VPN IP Address assignment methodology (DHCP/VPN pool) and click Next.
        v. Specify VPN pool if VPN pool was chosen in step d and click Next.
        vi. Identify the network that has shared access to the Internet and click Next.
        vii. Select if an external RADIUS server is to be used for central authentication and click Next.

    c. Give users VPN access rights. Open the properties page for a user, select that user's Dial-In properties page and select "Allow access" under Remote Access Permissions.

3. Configure Server Logging - Enable authentication and accounting logging from the **Settings** tab on the properties of the **Local File** object in the **Remote Access Logging** folder in the Routing and Remote Access snap-in. The authentication and accounting information is stored in a configurable log file or files stored in the *SystemRoot*\System32\LogFiles folder. The log files are saved in Internet Authentication Service (IAS) or database-compatible format, meaning that any database program can read the log file directly for analysis.
4. Configure Snare agent to send logs to FortiSIEM.

Sample Syslog Messages

```
<13>Apr  1 09:28:03 dev-v-win03-vc MSPPTPLog    0

192.168.24.11,administrator,04/01/2009,09:28:00,RAS,DEV-V-WIN03-
VC,44,29,4,192.168.24.11,6,2,7,1,5,129,61,5,64,1,65,1,31,192.168.20.38,66,192.168.20.38,4108
,192.168.24.11,4147,311,4148,MSRASV5.20,4155,1,4154,Use Windows authentication for all
users,4129,DEV-V-WIN03-VC\administrator,4130,DEV-V-WIN03-VC\administrator,4127,4,25,311 1
192.168.24.11 04/01/2009 16:12:12 3,4149,Connections to Microsoft Routing and Remote Access
server,4136,1,4142,0
```

Pulse Secure

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Security and Performance alerts	Security and performance monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "PulseSecure" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Syslog

Follow the Pulse Secure documentation to send syslog to FortiSIEM.

Sample PulseSecure Syslog Messages

```
<134> 2015-12-18T06:30:29-08:00  PulseSecure: 2015-12-18 06:30:29 - XXX-A1234-VPNSSL01 -
[1.1.1.1] admin(company1 Realm)[some title] - Host Checker policy 'VMS_Host_Checker_Policy'
passed on host '1.1.1.1' address ''  for user 'admin'.
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Pulse Secure Pulse Connect
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Vulnerability Scanners

FortiSIEM supports these vulnerability scanners for discovery and monitoring.

- AlertLogic
- Digital Defense Frontline Vulnerability Manager
- Green League WVSS
- McAfee Foundstone Vulnerability Scanner
- Qualys QualysGuard Scanner
- Qualys Vulnerability Scanner
- Rapid7 Nexpose Vulnerability Scanner (Vulnerability Management On-Premises)
- Rapid7 InsightVM (Platform Based Vulnerability Management)
- Tenable.io
- Tenable Nessus Vulnerability Scanner
- Tenable Security Center
- YXLink Vulnerability Scanner

AlertLogic Intrusion Detection and Prevention Systems (IPS)

- Integration Points
- Configuring AlertLogic for FortiSIEM API Access
- Configuring FortiSIEM for AlertLogic API Access

Integration Points

Protocol	Information Discovered	Used For
AlertLogic V3 API	Security Alerts created by AlertLogic	Security and Compliance

Configuring AlertLogic for FortiSIEM API Access

Contact AlertLogic for API access key. This must be entered in FortiSIEM in the next step.

Configuring FortiSIEM for AlertLogic API Access

1. Logon to FortiSIEM
2. Go to **ADMIN > Setup > Credentials**.
3. At **Step 1: Enter Credentials**, click **New** to create AlertLogic API credential:

For Access Protocol = AlertLogic API V3

Setting	Value
Name	<set name>
Device Type	Alert Logic IPS
Access Protocol	AlertLogic API V3
Pull Interval	5 minutes
Password config	See Password Configuration
API Key	The API Key for device access is provided by AlertLogic
Organization	Choose the Organization if it is an MSP deployment and the same credential is to be used for multiple customers

For Access Protocol = AlertLogic IPS

Settings	Description
Name	Enter a name for the credential
Device Type	Alert Logic IPS
Access Protocol	Alert Logic IPS
Pull Interval	The interval in which FortiSIEM will pull events from Alert Logic. Default is 5 minutes.
Access Key ID	Access key for your Alert Logic instance.
Secret Key	Secret key for your Alert Logic instance
Organization	The organization the device belongs to.
Description	Description of the device.

4. At **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter "alertlogic.com" in the **IP/Hostname** field.
   b. Select the name of the credential created in step 3 from the **Credentials** drop-down list.
   c. Click **Save**.
5. Select the entry in step 4 and click the **Test** drop-down list and select **Test Connectivity**. If it succeeds, then the credential is correct.
6. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from AlertLogic Cloud service using the AlertLogic V3 API.

To test for events received from AlertLogic:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the AlertLogic entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from AlertLogic in the last 15 minutes. You can modify the time interval to get more events.

Digital Defense Frontline Vulnerability Manager

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Log

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Frontline REST API		Host name, Vulnerability name, Vulnerability CVE ID, Vulnerability score, Operating system	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "Digital Defense" to see the event types associated with this device. In FortiSIEM 6.3.0, there are 3 event types defined.

Rules

There are no specific rules available for Digital Defense Frontline Vulnerability Manager, but the rule "Scanner found severe vulnerability" applies.

Reports

There are no specific reports available for Digital Defense Frontline Vulnerability Manager, but the report "Host vulnerabilities found by scanner" can be used.

Configuration

- Setup in Digital Defense Frontline Vulnerability Manager
- Setup in FortiSIEM

Setup in Digital Defense Frontline Vulnerability Manager

Complete these steps from the Frontline Vulnerability Manager Portal.

1. Log into Frontline VM.
2. In the site header, select your name and choose **My profile**.
3. On the **API Tokens** tab, select **Create new token**.
4. In the **Add New Token** dialog, enter a token name, and select **OK**. Your token should be created.
5. Below your token name, select **Click to show key** to display your API Key.
6. Copy this information for your Setup in FortiSIEM.

Setup in FortiSIEM

FortiSIEM processes events from the Vulnerability Manager via the Digital Defense API. Obtain your API Key from the Frontline Vulnerability Manager Portal before proceeding.

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**:
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box, and click **Save** when done.

Settings	Description
Name	Enter a name for the credential.
Device Type	Digital Defense Frontline Vulnerability Manager
Access Protocol	FRONTLINE_API
Pull Interval	5 minutes
Token	Input the API Key from your Digital Defense Frontline Vulnerability Manager API.
Confirm Token	Input the same API Key as above for verification.
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Select the name of your credential from the **Credentials** drop-down list. The **IP/Host Name** field should auto populate with "vm.frontline.cloud".
   b. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Digital Defense Frontline Vulnerability Manager.
5. To see the jobs associated with Digital Defense Frontline Vulnerability Manager, select **ADMIN > Setup > Pull Events**.
6. To see the received events select **ANALYTICS**, then enter "Frontline" in the search box.

Sample Logs

- Frontline-Scan-Finished
- Frontline-Vuln-Detected
- Frontline-Device-Vuln-Score

Frontline-Scan-Finished

```
{"ServerHostName":"vm.frontline.cloud","ServerIp":"54.196.81.232","account":
{"id":3516,"name":"Fortinet Integration Test"},"account_id":3516,"account_user":"Dan
Hanman","account_user_id":15006,"build_reports":false,"businessgroups":{},"date_
finished":"2021-04-05T23:27:05.004265Z","date_modified":"2021-04-05T23:27:05.146169Z","date_
started":"2021-04-05T23:27:03.489965Z","deleting":false,"description":"","exclude_from_
active_view":false,"force_target_detection":false,"has_results":false,"host_
count":0,"id":"298183_20210405T232500Z","is_rna_scan":true,"name":"Scan Mar 25, 2021
1:25PM","next_event":null,"phCustId":1,"scan_locations":"internal","scan_
policy":"Default","status":"completed","status_message":null,"status_
name":"Completed","workflow":"va_workflow"}
```

Frontline-Vuln-Detected

```
{"ServerHostName":"vm.frontline.cloud","ServerIp":"54.196.81.232","acceptable_
risk":null,"active_view_active_risk_details":null,"active_view_active_risk_
score":null,"active_view_date_created":null,"active_view_date_first_created":null,"active_
view_threat_rank":null,"analyst_threat_intel":null,"cve":"","cvss_base_score_v2":0.0,"cvss_
base_score_v3":null,"cvss_score":"0.0","cvss_version":"2.0","data":"Wordpress 4.0.6
detected","date_finished":null,"date_started":null,"detect_type":"remote","exploitability":
{"exploited_in_wild":null,"has_exploit_func":false,"has_exploit_kit":null,"has_exploit_
poc":null,"is_crimewareable":null,"is_exploitable":null,"is_priority_
exploitable":null},"false_positive":false,"has_notes":false,"hidden":false,"hide_from_now_
on":false,"host_hidden":false,"host_
id":85634681,"hostname":"172.23.177.67","id":3202200906,"id_ddi":102095,"ip_
address":"172.23.177.67","labels":[],"manually_added":false,"manually_added_date_fix_
confirmed":null,"manually_added_fix_status_name":null,"matched_
status":"new","phCustId":1,"port":80,"protocol":"http","scan_block_id":"548616","scan_
id":"277898","scan_version":1016281,"scan_version_active_risk_details":null,"scan_version_
active_risk_score":null,"scan_version_date_created":"2020-12-02T17:46:12.640112Z","scan_
version_host_id":85634681,"scan_version_threat_rank":null,"scan_version_vulnerability_
id":3202200906,"scanner_version":"3.0.26.2","severities":{"ddi":"info","ddi_
alt":"trivial","nvd":"low","nvd_alt":"low","pci":"pass","pci_alt":"pass"},"threat_activity":
{"1m":0,"1w":0,"1y":0,"3m":0,"total":0},"title":"Wordpress
Detected","transport":"tcp","tunnel":"none","vuln_class":"explicit"}
```

Frontline-Device-Vuln-Score

```
{"ServerHostName":"vm.frontline.cloud","ServerIp":"54.196.81.232","active_view_active_risk_
details":{"ars_unweighted":92.024999999999991,"exposure_score":{"domain":"WIN-
30QQRC10MGG","domain_host_count":4,"domain_threat_rank":95.0,"external_
asset":false,"subnet":null,"subnet_host_count":0,"subnet_threat_
rank":0,"unweighted":68.5,"weight":0.050000000000000003,"weighted":3.4250000000000003},"ris
k_weight":{"host_risk_weight":50.0},"severity_score":
{"unweighted":84,"weight":0.14999999999999999,"weighted":12.6},"threat_score":
{"unweighted":95.0,"weight":0.80000000000000004,"weighted":76.0}},"active_view_cvss_
version":2.0,"active_view_date_created":"2020-12-02T17:46:12.640112Z","active_view_date_
first_created":"2020-12-02T17:46:12.640112Z","agent_uuid":null,"assessed_cis_
auth":false,"assessed_db_auth":false,"assessed_os_auth":false,"assessed_threatscan_
auth":true,"assessed_unauth":true,"auth_status":{"details":{},"extended_details":
{"cis":null,"db":{"mssql":null,"mysql":null,"oracle":null,"postgresql":null},"os":
{"linux":null,"vmware":null,"windows":null},"threatscan":"Threat Scan completed
successfully"},"overall":"N/A"},"aws_instance_id":null,"base_scan_id":"277898","date_
finished":null,"date_started":null,"discovery_method":"nbname","dns_name":"","dns_
smartname":"WIN-30QQRC10MGG","has_antivirus":true,"has_crimewareable":null,"has_disabled_
antivirus":false,"has_exploitable":null,"has_malware":false,"has_notes":false,"has_outdated_
antivirus":false,"hidden":false,"hide_from_now_on":false,"hostname":"WIN-
30QQRC10MGG","id":85634671,"internal":true,"ip_address":"172.23.177.55","is_
compromised":false,"is_retired":false,"labels":[{"color":"blue","deleted":false,"display_
name":"WIN-30QQRC10MGG","id":214189,"labeled_by":0,"location":1}],"mac_
address":"00:50:56:8d:16:52","matched_status":"new","named_asset_name":null,"netbios_
name":"WIN-30QQRC10MGG","netbios_smartname":"WIN-30QQRC10MGG","network_profile_
id":7286,"network_profile_name":"Internal Scanner Profile","notes_distribution":
{"asset":false,"asset_only":false,"vuln_only":false},"os":"Windows Server 2012 R2
Standard","os_family":"windows","os_type":"server","partially_scanned":false,"pentest_
status":null,"phCustId":1,"scan_block_id":"548616","scan_id":"277898","scan_
version":1016281,"scan_version_active":true,"scan_version_active_risk_details":{"ars_
unweighted":92.024999999999991,"exposure_score":{"domain":"WIN-30QQRC10MGG","domain_host_
count":4,"domain_threat_rank":95.0,"external_asset":false,"subnet":null,"subnet_host_
count":0,"subnet_threat_
rank":0,"unweighted":68.5,"weight":0.050000000000000003,"weighted":3.4250000000000003},"ris
k_weight":{"host_risk_weight":50.0},"severity_score":
```

```
{"unweighted":84,"weight":0.14999999999999999,"weighted":12.6},"threat_score":
{"unweighted":95.0,"weight":0.80000000000000004,"weighted":76.0}},"scan_version_active_risk_
score":92.025000000000006,"scan_version_cvss_score":10.0,"scan_version_cvss_
version":2.0,"scan_version_date_created":"2020-12-02T17:46:12.640112Z","scan_version_host_
id":85634671,"scan_version_host_rating_list":{"ddi":"D","ddi_alt":"F","nvd":"High","nvd_
alt":"High","pci":"Fail","pci_alt":"Fail"},"scan_version_host_severity_list":
{"ddi":"high","nvd":"high","pci":"fail"},"scan_version_risk_score":175.0,"scan_version_risk_
weight":50.0,"scan_version_threat_rank":95.0,"scan_version_vulnerability_count":29,"scan_
version_vulnerability_severity_counts":{"unweighted":{"ddi":{"counts":
{"critical":0,"high":1,"info":21,"low":0,"medium":1,"none":0,"trivial":6},"overall_security_
gpa":1.0},"ddi_alt":{"counts":
{"critical":1,"high":1,"info":0,"low":1,"medium":0,"none":0,"trivial":26},"overall_security_
gpa":0},"nvd":{"counts":{"high":2,"low":24,"medium":3},"overall_security_gpa":0},"nvd_alt":
{"counts":{"high":1,"low":27,"medium":1},"overall_security_gpa":0},"pci":{"counts":
{"fail":2,"pass":27},"overall_security_gpa":0},"pci_alt":{"counts":
{"fail":2,"pass":27},"overall_security_gpa":0}},"weighted":{"ddi":{"counts":
{"critical":0,"high":1,"info":21,"low":0,"medium":1,"none":0,"trivial":6},"overall_security_
gpa":1.0},"ddi_alt":{"counts":
{"critical":1,"high":1,"info":0,"low":1,"medium":0,"none":0,"trivial":26},"overall_security_
gpa":0},"nvd":{"counts":{"high":2,"low":24,"medium":3},"overall_security_gpa":0},"nvd_alt":
{"counts":{"high":1,"low":27,"medium":1},"overall_security_gpa":0},"pci":{"counts":
{"fail":2,"pass":27},"overall_security_gpa":0},"pci_alt":{"counts":
{"fail":2,"pass":27},"overall_security_gpa":0}}},"scanner_version":"3.0.26.2"}
```

Green League WVSS (Web Application Vulnerability Scanning System)

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in “Setting Credentials“ in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Green League WVSS
Access Protocol	WVSS API
Pull Interval	60 minutes
Domain	Domain name
User Name	User name for device access
Password	Password for device access
Description	Description of the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Green League WVSS.
5. To see the jobs associated with Green League, navigate to **ADMIN > Setup > Pull Events**.To see the received events, navigate to **ANALYTICS**, then enter "Green League" in the search box.

McAfee Foundstone Vulnerability Scanner

What is Discovered and Monitored

Protocol	Metrics collected	Used for
JDBC (SQL Server)	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulerability CVE Id, Vulnerability Score, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "mcafee-vul" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined rules for this device.

Configuration

JDBC

FortiSIEM connects to the `faultline` database in the McAfee vulnerability scanner to collect metrics. This is a SQL Server database, so you must have set up access credentials for the database over JDBC to set up access credentials in FortiSIEM and initiate discovery.

Settings for Access Credentials

Settings for McAfee Foundstone Vulnerability Scanner JDBC Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	mcafee_jdbc
Device Type	Microsoft SQL Server
Access Protocol	JDBC
Used for	McAfee VulnMgr
Pull Interval (minutes)	5
Port	1433
Database name	faultline
User Name	A user with access to the faultline database over JDBC
Password	The password associated with the user

Qualys QualysGuard Scanner

- Configuration in FortiSIEM

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	Qualys QualysGuard Scanner
Access Protocol	Qualys API
Pull Interval	60 minutes
Port	443
User Name	A user who has access to the vulnerability scanner over the API.
Password	Password associated with the user
Description	Description about the device

3. In **Step 2, Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential created in step 2 from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to Qualys QualysGuard Scanner.
5. To see the jobs associated with Qualys, select **ADMIN > Setup > Pull Events**.
6. To see the received events ,select **ANALYTICS**, then enter "Qualys" in the search box.

Qualys Vulnerability Scanner

What is Discovered and Monitored

Protocol	Metrics collected	Used for
Qualys API	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulerability CVE Id and Bugtraq Id, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "qualys" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "qualys" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

Qualys API

Create a user name and password that FortiSIEM can use as access credentials for the API.

You can configure FortiSIEM to communicate with your device, and then initiate discovery of the device. . For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Use Host Name for IP Range in Access Credentials

Enter the host name for your Qualys service rather than an IP address when associating your access credentials to an IP range.

Settings for Qualys Vulnerability Scanner API Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	qualys
Device Type	Qualys QualysGuard Scanner
Access Protocol	Qualys API
Pull Interval (minutes)	5
Port	443
User Name	A user who has access to the vulnerability scanner over the API
Password	The password associated with the user

Rapid7 Nexpose Vulnerability Scanner (Vulnerability Management On-Premises)

What is Discovered and Monitored

Protocol	Metrics collected	Used for
Rapid7 Nexpose API	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "rapid7" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Rapid7 Nexpose API

1. Log into the device manger for your vulnerability scanner with administrative credentials.
2. Go to **Administration > General > User Configuration**, and create a user that FortiSIEM can use to access the device.
3. Go to **Reports > General > Report Configuration**.
4. Create a report with the Report Format set to **Simple XML Report Version 1.0** or **NeXpose XML Report Version 2.0**.
   FortiSIEM can pull reports only in these formats.

Settings for Access Credentials

Settings for Rapid7 Nexpose API Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Rapid7 NeXpose Security Scanner
Access Protocol	Rapid7 NeXpose API
Pull Interval (minutes)	60
Port	3780
User Name	A user who can access the device over the API
Password	The password associated with the user

Rapid7 InsightVM Integration (Vulnerability Management On-Premises)

- Integration Points
- Rapid7 InsightVM API Integration
- Configuration

Integration Points

Protocol	Information collected	Used For
InsightVM API	Vulnerability scan data	Security and Compliance

Rapid7 InsightVM API Integration

FortiSIEM can pull vulnerability scan data from Rapid7 InsightVM Server via InsightVM API.

InsightVM scan data contains vulnerabilities found on a host. Each host vulnerability is converted into a separate FortiSIEM event with event type Rapid7-InsightVM-Vuln-Detected.

Configuration

- Configuring Rapid7 InsightVM Server
- Configuring FortiSIEM

Configuring Rapid7 InsightVM Server

Create an account to be used for FortiSIEM communication.

Configuring FortiSIEM

Use the account in previous step to enable FortiSIEM access:

Define Rapid7 Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
1. b. Enter these settings in the Access Method Definition dialog box and click **Save**.

Settings	Description
Name	Enter a name for the credential
Device Type	Rapid7 InsightVM
Access Protocol	InsightVM API
Pull Interval	Choose the Pull Interval (Default 60 minutes). Fortinet recommends 5 minutes for general cases.
Port	Choose the HTTPS Port (default 3780).
User Name	Enter the **User Name** for the account created while Configuring Rapid7 InsightVM Server.
Password	Enter the **Password** for the account created while Configuring Rapid7 InsightVM Server.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter the IP address of the Rapid7 Insight VM Server in the **IP/Host Name** field.
   b. Select the name of the credential created in Define Rapid7 Credential in FortiSIEM from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. Go to **ADMIN > Setup > Discovery**, click **New**, fill out the information and ensure you input the IP address used in Step 1a, and click **Save**.
4. Click **Discover** and confirm it succeeds.
5. An entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Rapid7 InsightVM Server using the InsightVM REST API.

To test for received InsightVM Vulnerability events:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the InsightVM entry and click **Report**.

The system will take you to the **ANALYTICS** tab and run a query to display the events received from InsightVM Server in the last 15 minutes. You can modify the time interval to get more events.

Tenable.io

- Integration Points
- Tenable.io API Integration
- Configuration

Integration Points

Protocol	Logs Collected	Used For
Tenable.io API	Vulnerability scan data	Security and Compliance

Tenable.io API Integration

FortiSIEM can pull vulnerability scan data from Tenable.io Cloud Service via Tenable.io API.

Tenable.io scan data contains vulnerabilities found on a host. Each host vulnerability is converted into a separate FortiSIEM event with event type TenableIO-Vuln-Detected.

Configuration

- Configuring Tenable.io Cloud Service
- Configuring FortiSIEM

Configuring Tenable.io Cloud Service

Create an API Key to be used for FortiSIEM communication.

1. Login to your Tenable.io portal using your account.
2. Create API Key for use in FortiSIEM:
   a. For administrative user.
   b. Click **Settings** > **User**.
   c. In **User** table, click the name of the **User** you want to edit.
   d. Click the **API Keys** tab in the generate and click **Generate**.
   e. Click **Save**.
3. For regular user:
   a. Click **My Account**.
   b. Click the **API Keys** tab in the generate and click **Generate**.
   c. Click **Save**.

Configuring FortiSIEM

Define Tenable.io Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Tenable Tenable.io
Access Protocol	TenableIO API
Pull Interval	Choose the Pull Interval (Default 60 minutes). Fortinet recommends 5 minutes for general cases.
Account	Enter the **Account** obtained from Tenable.io portal (see Configuring Tenable.io Cloud Service).
Access Key	Enter the **Access Key** obtained from Tenable.io portal (see Configuring Tenable.io Cloud Service).
Secret Key	Enter the **Secret Key** obtained from Tenable.io portal (see Configuring Tenable.io Cloud Service).
Organization	Choose the **Organization** if it is an MSP deployment and the same credential is to be used for multiple customers.
Description	Description of the device.

Create IP Range to Credential Association and Test Connectivity

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter "cloud.tenable.com" in the **IP/Host Name** field.
   b. Select the name of the credential created in Define Tenable.io Credential in FortiSIEM from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results. After **Test Connectivity** succeeds, an entry will be created in

ADMIN > Setup > Pull Events corresponding to this event pulling job. FortiSIEM will start to pull events from Tenable.io portal using the API.

To test for received Tenable.io events:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the Tenable.io entry and click **Report**.
3. The system will take you to the **ANALYTICS** tab and run a query to display the events received from Tenable.io in the last 15 minutes. You can modify the time interval to get more events.

Tenable Nessus Vulnerability Scanner

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration

What is Discovered and Monitored

Protocol	Metrics collected	Used for
Nessus API	Scan name, Scanned Host Name, Host OS, Vulnerability category, Vulnerability name, Vulnerability severity, Vulerability CVE Id and Bugtraq Id, Vulnerability CVSS Score, Vulnerability Consequence	Security Monitoring

Event Types

In **ADMIN > Device Support > Event Types**, search for "nessus" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "nessus" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

To configure a Tenable Nessus Security Scanner, take the following steps:

1. Deploy a Nessus server (5, 6, 7, or 8).
2. Generate an API key. For Nessus 7 or Nessus 8, obtain the Access Key and Secret Key.
   Note: If using Nessus (5) or Nessus 6, create a username and password that FortiSIEM can use to access the API and make sure the user has permissions to view the scan report files on the Nessus device. You can check if your user has the right permissions by running a scan report as that user.
3. Add a target device IP that will be scanned.
4. Login to the FortiSIEM GUI.
5. Navigate to **CMDB > Devices**.
6. Add the target device IP to **CMDB > Devices** in FortiSIEM.
7. Navigate to **ADMIN > Setup**, and click the **Credentials** tab.

8. In **Step 1: Enter Credentials**, click **New**:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these Nessus credential settings in the Access Method Definition dialog box and click **Save**:

Setting	Value
Name	<set name>
Device Type	Choose the appropriate device type: -Tenable Nessus Security Scanner -Tenable Nessus6 Security Scanner -Tenable Nessus7 Security Scanner -Tenable Nessus8 Security Scanner
Access Protocol	The access protocol will auto populate based off the device type selected: -Nessus API -Nessus6 API -Nessus7 API -Nessus8 API
Pull Interval (minutes)	5 (default 60 minutes)
Port	8834
User Name (for Nessus and 6)	A user who has permission to access the device over the API
Password (for Nessus and 6)	The password associated with the user
Access Key (for Nessus7 and 8)	Obtain the Access Key from Nessus
Secret Key (for Nessus7 and 8)	Obtain the Secret Key from Nessus

9. In **Step 2: Enter IP Range to Credential Associations**, click **New**.
   a. Select the credential you created earlier from the **Credentials** drop-down list.
   b. In the **IP/Host Name** field, enter the IP/IP Range or Host Name.
   c. Click **Save**.
10. Select the new mapping and click the **Test** drop-down list and select **Test Connectivity without Ping** to start the polling.
11. Navigate to **ADMIN > Setup > Pull Events.** The yellow star besides the Nessus pull job should turn the color green.
12. Scan the target device IP in the Nessus server, and export the scan report.
13. Navigate to **ANALYTICS** in FortiSIEM, and query the Nessus events with the condition `Event Type = Nessus-Vuln-Detected`.
14. Compare the events in the FortiSIEM with the scan report exported from the Nessus server.

Note that the severity matching rule between Nessus8 and AO Event are as follows:

Nessus Status	FortiSIEM Event Severity Number
Critical	Event Severity 10
High	Event Severity 9
Medium	Event Severity 6
Low	Event Severity 2
None	Event Severity 3

If Vulnerability CVE ID in FortiSIEM events is not `NULL`, the target device IP will be added to **INCIDENTS > Risk** in FortiSIEM.

Tenable Security Center

- Integration Points
- Tenable.sc (Security Center) API Integration
- Configuration
- Sample Events

Integration Points

Protocol	Information collected	Used for
Tenable.sc API	Vulnerability scan data	Security and Compliance

Tenable.sc (Security Center) API Integration

FortiSIEM can pull vulnerability scan data via the Tenable.sc API.

Tenable.sc scan data contains vulnerabilities found on a host. Each host vulnerability is converted into a separate FortiSIEM event with event type TenableSC-Vuln-Detected.

Configuration

- Configuring Tenable.sc for FortiSIEM
- Configuring FortiSIEM

Configuring Tenable.sc for FortiSIEM

Except for setting your Tenable account user name and password, no special configuration is needed for Tenable.sc.

Configuring FortiSIEM

Use the API Key and Secret in the previous step to enable FortiSIEM access.

- Define Tenable Security Center Credential in FortiSIEM
- Create IP Range to Credential Association, Test Connectivity and Pull Events

Define Tenable Security Center Credential in FortiSIEM

Complete these steps in the FortiSIEM UI by first logging in to the FortiSIEM Supervisor node.

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential:
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box and click **Save**:

1.

Settings	Description
Name	Enter a name for the credential
Device Type	Tenable Tenable Security Center
Access Protocol	Tenable.sc API
Pull Interval	Choose the Pull Interval (Default 60 minutes).
Port	Enter the **Port** number. (Default 443)
User Name	Enter the **User Name** for the Tenable Security Center account.
Password	Enter the **Password** for the Tenable Security Center user name account.
Description	Description of the device.

Create IP Range to Credential Association, Test Connectivity and Pull Events

From the FortiSIEM Supervisor node, take the following steps (In **ADMIN > Setup > Credentials**).

1. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a mapping.
   a. Enter the host's IP address or host name in the **IP/Host Name** field.
   b. Select the name of the credential created in Define Tenable Security Center Credential in FortiSIEM from the **Credentials** drop-down list.
   c. Click **Save**.
2. Select the entry just created and click the **Test** drop-down list and select **Test Connectivity without Ping**. A pop up will appear and show the Test Connectivity results.
3. After **Test Connectivity** succeeds, an entry will be created in **ADMIN > Setup > Pull Events** corresponding to this event pulling job. FortiSIEM will start to pull events from Tenable Security Center using the API.

To test for received Tenable.sc events:

1. Go to **ADMIN > Setup > Pull Events**.
2. Select the Tenable.sc entry and click **Report**.
3. The system will take you to the **ANALYTICS** tab and run a query to display the events received from Tenable.sc in the last 15 minutes. You can modify the time interval to get more events.

Sample Events

```
[TenableSc-Vuln-Detected]:[serverIp]=10.10.10.79,[serverName]=sc.tenalab.online,
[scanName]=tensc_job1__ordr_1580449845796,[endTime]=1580538767,[policyName]=6e8a5582-
076f-5798-b0c3-5384b8854cad-501013/Advanced Scan (Vulnerability),[osName]=linux,
[hostMACAddr]=00:16:3E:5D:7A:71,[osVersion]=Linux Kernel 2.6,[hostName]=target-
cent7.lxd,[hostIpAddr]=10.238.64.9,[startTime]=1580538643,[appPort]=22,
[appTransportProto]=tcp,[eventSeverity]=1,[nessusPluginId]=70658,[nessusPluginName]=SSH
Server CBC Mode Ciphers Enabled,[categoryType]=Misc.,[vulnCVEId]=CVE-2008-5161,
[vulnCvssBaseScore]=2.6,[vulnCvssBaseTemporal]=1.9,[cweId]=200,[vulnDesc]=The SSH
server is configured to support Cipher Block Chaining (CBC) encryption. This may allow
an attacker to recover the plaintext message from the ciphertext. Note that this plugin
```

```
only checks for the options of the SSH server and does not check for vulnerable
software versions.,[fileName]=ssh_cbc_supported_ciphers.nasl,[vulnType]=remote,
[threatLevel]=Low,[vulnSolution]=Contact the vendor or consult product documentation to
disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.,
[vulnCVESummary]=The SSH server is configured to use Cipher Block Chaining.,
[nessusPluginOutput]= The following client-to-server Cipher Block Chaining (CBC)
algorithms are supported : 3des-cbc aes128-cbc aes192-cbc aes256-cbc blowfish-cbc
cast128-cbc The following server-to-client Cipher Block Chaining (CBC) algorithms are
supported : 3des-cbc aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc
```

```
[TenableSc-Vuln-Detected]:[serverIp]=52.170.35.79,[serverName]=sc.tenalab.online,
[scanName]=tensc_job1__ordr_1580449845796,[endTime]=1580538767,[policyName]=6e8a5582-
076f-5798-b0c3-5384b8854cad-501013/Advanced Scan (Vulnerability),[osName]=linux,
[hostMACAddr]=00:16:3E:5D:7A:71,[osVersion]=Linux Kernel 2.6,[hostName]=target-
cent7.lxd,[hostIpAddr]=10.238.64.9,[startTime]=1580538643,[appPort]=0,
[appTransportProto]=tcp,[eventSeverity]=0,[nessusPluginId]=35081,[nessusPluginName]=Xen
Guest Detection,[categoryType]=Misc.,[vulnDesc]=According to the MAC address of its
network adapter, the remote host is a Xen virtual machine.,[fileName]=xen_detect.nasl,
[vulnType]=combined,[threatLevel]=None,[vulnSolution]=Ensure that the host's
configuration is in agreement with your organization's security policy.,
[vulnCVESummary]=The remote host is a Xen virtual machine.
```

YXLink Vuln Scanner

- Configuration in FortiSIEM

Configuration in FortiSIEM

Complete these steps in the FortiSIEM UI:

1. Go to the **ADMIN > Setup > Credentials** tab.
2. In **Step 1: Enter Credentials**, click **New** to create a new credential.
   a. Follow the instructions in "Setting Credentials" in the User's Guide to create a new credential.
   b. Enter these settings in the Access Method Definition dialog box:

Settings	Description
Name	Enter a name for the credential.
Device Type	YXLink Vuln Scanner
Access Protocol	YX API
Pull Interval	60 minutes
Port	0
Domain	Domain name
Description	Description about the device

3. In **Step 2: Enter IP Range to Credential Associations**, click **New** to create a new mapping.
   a. Enter a host name, an IP, or an IP range in the **IP/Host Name** field.
   b. Select the name of your credential from the **Credentials** drop-down list.
   c. Click **Save**.
4. Click the **Test** drop-down list and select **Test Connectivity** to test the connection to the YXLink Vulnerability Scanner.
5. To see the jobs associated with YXLink, select **ADMIN > Setup > Pull Events**.
6. To see the received events, select **ANALYTICS**, then enter "YXLink" in the search box.

WAN Accelerators

FortiSIEM supports these wide area network accelerators for discovery and monitoring.

- Cisco Wide Area Application Server
- Riverbed SteelHead WAN Accelerator

Cisco Wide Area Application Server

- What is Discovered and Monitored on page 838
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Software version, Hardware model, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Disk space utilization, Process cpu/memory utilization	Availability and Performance Monitoring

Event Types

Regular monitoring events

- PH_DEV_MON_SYS_UPTIME

  ```
  [PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
  [lineNumber]=1053,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,[sysUpTime]=13256948,
  [sysUpTimePct]=100.000000,[sysDownTime]=0,[pollIntv]=56,[phLogDetail]=
  ```

- PH_DEV_MON_SYS_CPU_UTIL

  ```
  [PH_DEV_MON_SYS_UPTIME]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
  [lineNumber]=1053,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,[sysUpTime]=13256948,
  [sysUpTimePct]=100.000000,[sysDownTime]=0,[pollIntv]=56,[phLogDetail]=
  ```

- PH_DEV_MON_SYS_MEM_UTIL

  ```
  [PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
  [lineNumber]=9822,[memName]=Physical Memory,[hostName]=edge.bank.com,
  [hostIpAddr]=10.19.1.5,[memUtil]=93.438328,[pollIntv]=176,[phLogDetail]=
  ```

- PH_DEV_MON_SYS_DISK_UTIL

  ```
  [PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
  [lineNumber]=9902,[diskName]=/swstore,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,
  [appTransportProto]=SNMP (hrStorage),[diskUtil]=56.931633,[totalDiskMB]=992,
  [usedDiskMB]=565,[freeDiskMB]=427,[pollIntv]=176,[phLogDetail]=
  ```

- PH_DEV_MON_SYS_PROC_COUNT

```
[PH_DEV_MON_SYS_PROC_COUNT]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=11710,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,[procCount]=429,
[pollIntv]=176,[phLogDetail]=
```

- PH_DEV_MON_NET_INTF_UTIL

```
 [PH_DEV_MON_NET_INTF_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phIntfFilter.cpp,
[lineNumber]=323,[intfName]=GigabitEthernet 1/0,[intfAlias]=,[hostName]=edge.bank.com,
[hostIpAddr]=10.19.1.5,[pollIntv]=56,[recvBytes64]=0,[recvBitsPerSec]=0.000000,
[inIntfUtil]=0.000000,[sentBytes64]=0,[sentBitsPerSec]=0.000000,[outIntfUtil]=0.000000,
[recvPkts64]=0,[sentPkts64]=0,[inIntfPktErr]=0,[inIntfPktErrPct]=0.000000,
[outIntfPktErr]=0,[outIntfPktErrPct]=0.000000,[inIntfPktDiscarded]=0,
[inIntfPktDiscardedPct]=0.000000,[outIntfPktDiscarded]=0,
[outIntfPktDiscardedPct]=0.000000,[outQLen64]=0,[intfInSpeed64]=100000000,
[intfOutSpeed64]=100000000,[intfAdminStatus]=,[intfOperStatus]=,[daysSinceLastUse]=0,
[totIntfPktErr]=0,[totBitsPerSec]=0.000000,[phLogDetail]=
```

- PH_DEV_MON_PROC_RESOURCE_UTIL

```
[PH_DEV_MON_PROC_RESOURCE_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=phPerfJob.cpp,
[lineNumber]=4320,[swProcName]=syslogd,[hostName]=edge.bank.com,[hostIpAddr]=10.19.1.5,
[procOwner]=,[memUtil]=0.038191,[cpuUtil]=0.000000,[appName]=Syslog Server,
[appGroupName]=Unix Syslog Server,[pollIntv]=116,[swParam]=-s -f /etc/syslog.conf-
diamond,[phLogDetail]=
```

Rules

Regular monitoring rules

Reports

Regular monitoring reports

Configuration

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Cisco WAAS
Access Protocol	See Access Credentials
Port	See Access Credentials

Setting	Value
Password config	See Password Configuration

Riverbed SteelHead WAN Accelerator

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Host name, Software version, Hardware model, Network interfaces	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Disk space utilization, Process cpu/memory utilization	Availability and Performance Monitoring
SNMP		Hardware status	Availability and Performance Monitoring
SNMP		**Bandwidth metrics**: Inbound Optimized Bytes - LAN side, WAN side, Outbound optimized bytes - LAN side and WAN side **Connection metrics**: Optimized connections, Passthrough connections, Half-open optimized connections, Half-closed Optimized connections, Established optimized connections, Active optimized connections **Top Usage metrics**: Top source (Source IP, Total Bytes), Top destination (Destination IP, Total Bytes), Top Application (TCP/UDP port, Total Bytes), Top Talker (Source IP, Source Port, Destination IP, Destination Port, Total Bytes) **Peer status**: For every peer: State, Connection failures, Request timeouts, Max latency	Availability and Performance Monitoring
SNMP Trap		All traps: software errors, hardware errors, admin login, performance issues - cpu, memory, peer latency issues. About 115 traps defined in ADMIN > Device Support > Event. The mapped event types start with "Riverbed-".	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "steelhead" to see the event types associated with this device.

Rules

In **RESOURCES > Rules**, search for "steelhead" in the main content panel **Search...** field to see the rules associated with this device.

Reports

There are no predefined reports for this device.

Configuration

- SNMP
- SNMP Trap

SNMP

FortiSIEM uses SNMP to discover and monitor this device. Make sure SNMP is enabled for the device as directed in its product documentation. For more information, refer to sections "Discovery Settings" and "Setting Credentials" in the User Guide.

SNMP Trap

FortiSIEM processes events from this device via SNMP traps sent by the device. Configure the device to send send SNMP traps to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Riverbed Steelhead
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Wireless LANs

FortiSIEM supports these wireless local area network devices for discovery and monitoring.

- Aruba Networks Wireless LAN
- Cisco Wireless LAN
- CradlePoint
- FortiAP
- FortiWLC
- Motorola WiNG WLAN AP
- Ruckus Wireless LAN

Aruba Networks Wireless LAN

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

FortiSIEM uses SNMP and NMAP to discover the device and to collect logs and performance metrics. FortiSIEM communicates to the WLAN Controller only and discovers all information from the Controller. FortiSIEM does not communicate to the WLAN Access points directly.

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller host name, Controller hardware model, Controller network interfaces, Associated WLAN Access Points	Controller Uptime, Controller Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Radio interface performance metrics	Availability and Performance Monitoring
SNMP Trap	Controller device type	All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "aruba" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **RESOURCES > Reports**, search for "aruba" in the main content panel **Search...** field to see the reports associated with this device.

Configuration

SNMP V1/V2c

1. Log in to your Aruba wireless controller with administrative privileges.
2. Go to **Configuration > Management > SNMP**.
3. For **Read Community String**, enter `public`.
4. Select **Enable Trap Generation**.
5. Next to **Read Community String**, click **Add**.
6. Under **Trap Receivers**, click **Add** and enter the IP address of your FortiSIEM virtual appliance.

Sample Aruba Networks Wireless LAN Controller SNMP Trap Messages

```
2008-06-11 11:38:34 192.168.20.7 [192.168.20.7]:SNMPv2-MIB::sysUpTime.0 = Timeticks:
(1355400) 3:45:54.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.14823.2.2.1.1.100.1003 SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.60 =
Hex-STRING: 07 D8 06 0B 13 2E 39 00 2D 07 00 SNMPv2-
SMI::enterprises.14823.2.2.1.1.2.1.1.2.192.168.180.1 = Hex-STRING: 00 1E 52 72 AF 4B
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Aruba ArubaOS WLAN AP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Cisco Wireless LAN

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller host name, Controller hardware model, Controller network interfaces, Associated WLAN Access Points	Controller Uptime, Controller CPU and Memory utilization, Controller Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths)	Availability and Performance Monitoring
SNMP Trap	Controller device type	All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health	Availability, Security and Compliance

Event Types

In **ADMIN > Device Support > Event Types**, search for "cisco wireless" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP V1/V2c and SNMP Traps

1. Log in to your Cisco wireless LAN controller with administrative privileges.
2. Go to **MANAGEMENT > SNMP > General**.
3. Set both **SNMP v1 Mode** and **SNMP v2c Mode** to **Enable**.
4. Go to **SNMP > Communities**.
5. Click **New** and create a `public` community string with **Read-Only** privileges.
6. Click **Apply**.
7. Go to **SNMP > Trap Controls**.
8. Select the event traps you want to sent to FortiSIEM.
9. Click **Apply**.
10. Go to **SNMP > Trap Receivers**.
11. Click **New** and enter the IP address of your FortiSIEM virtual appliance as a trap receiver.
12. Click **Apply**.

Sample SNMP Trap

```
2008-06-09 08:59:50 192.168.20.9 [192.168.20.9]:SNMPv2-MIB::sysUpTime.0 = Timeticks:
(86919800) 10 days, 1:26:38.00     SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.14179.2.6.3.2  SNMPv2-SMI::enterprises.14179.2.6.2.35.0 = Hex-STRING: 00 21
55 4D 66 B0        SNMPv2-SMI::enterprises.14179.2.6.2.36.0 = INTEGER: 0   SNMPv2-
SMI::enterprises.14179.2.6.2.37.0 = INTEGER: 1   SNMPv2-SMI::enterprises.14179.2.6.2.34.0 =
Hex-STRING: 00 12 F0 0A 3F 15

2010-11-01 12:59:57 0.0.0.0(via UDP: [172.22.2.25]:32769) TRAP2, SNMP v2c, community 1n3t3ng
. Cold Start Trap (0) Uptime: 0:00:00.00 DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks:
(9165100) 1 day, 1:27:31.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.9.9.599.0.4 SNMPv2-SMI::enterprises.9.9.599.1.3.1.1.1.0 = Hex-STRING: 00 24
D7 36 A0 00  SNMPv2-SMI::enterprises.9.9.513.1.1.1.1.5.0 = STRING: "AP-2" SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.8.0 = Hex-STRING: 00 25 45 B7  66 70  SNMPv2-
SMI::enterprises.9.9.513.1.2.1.1.1.0 = INTEGER: 0 SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.10.0 = IpAddress: 172.22.4.54 SNMPv2-
SMI::enterprises.9.9.599.1.2.1.0 = STRING: "IE\brouse" SNMPv2-
SMI::enterprises.9.9.599.1.2.2.0 = STRING: "IE"2011-04-05 10:37:42 0.0.0.0(via UDP:
[10.10.81.240]:32768) TRAP2, SNMP v2c, community FortiSIEM      . Cold Start Trap (0) Uptime:
0:00:00.00 DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1672429600) 193 days,
13:38:16.00     SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.9.9.615.0.1 SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.1.0 = Hex-STRING: 00 25 BC 80 E8 77    SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.8.0 = Hex-STRING: 6C 50 4D 7D AC 50    SNMPv2-
SMI::enterprises.9.9.599.1.3.1.1.9.0 = INTEGER: 1 SNMPv2-
SMI::enterprises.9.9.513.1.1.1.1.5.0 = STRING: "AP03-3.rdu2" SNMPv2-
SMI::enterprises.9.9.615.1.2.1.0 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.615.1.2.2.0 =
INTEGER: 5000 SNMPv2-SMI::enterprises.9.9.615.1.2.3.0 = INTEGER: 1 SNMPv2-
SMI::enterprises.9.9.615.1.2.4.0 = INTEGER: 31 SNMPv2-SMI::enterprises.9.9.615.1.2.5.0 =
INTEGER: -60 SNMPv2-SMI::enterprises.9.9.615.1.2.6.0 = INTEGER: -90 SNMPv2-
SMI::enterprises.9.9.615.1.2.7.0 = STRING:
"0,0,0,0,1,20,24,28,3,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0" SNMPv2-
SMI::enterprises.9.9.615.1.2.8.0 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.615.1.2.9.0 =
STRING: "6c:50:4d:7d:ac:50,e8:04:62:0b:b5:f0" SNMPv2-SMI::enterprises.9.9.615.1.2.10.0 =
STRING: "-83,-85" SNMPv2-SMI::enterprises.9.9.615.1.2.11.0 = STRING: "1,1" SNMPv2-
SMI::enterprises.9.9.512.1.1.1.1.11.5 = INTEGER: 1
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>
Device Type	Generic
Access Protocol	SNMP
Community String	<your own>

CradlePoint

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **ADMIN > Device Support > Event Types**, search for "CradlePoint" to see the event types associated with this application or device.

Rules

No specific rules are written for CradlePoint, but generic rules for Firewall, VPN Gateway, WLAN AP, Router Switch apply where there are matching event types.

Reports

No specific reports are written for CradlePoint, but generic reports for Firewall, VPN Gateway, WLAN AP, Router Switch apply where there are matching event types.

Configuration

Configure syslog forwarding of event information from CradlePoint.

Settings for Access Credentials

None required.

Sample Events

```
<14>(host) dhcp: Updated DHCP client: hostname 10.4.42.222 58:94:6b:8d:2b:94
```

FortiAP

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Sample Events
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP (to FortiGate)	Access point – Name, OS, Interfaces, Controller (FortiGate)	FortiAP CPU, Memory, Clients, Sent/Received traffic	Performance and Availability Monitoring
Syslog (from FortiGate)	Wireless events		Security and Log Analysis

FortiAPs are discovered from FortiGate firewalls via SNMP. FortiAP logs are received via FortiGate firewalls.

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiGate-Wireless" and “FortiGate-event” to see the event types associated with this device.

Rules

There are generic rules that trigger for this device as event types are mapped to specific event type groups.

Reports

Generic reports are written for this device as event types are mapped to specific event type groups.

Configuration

Configure FortiGate to:

1. Send Syslog to FortiSIEM.
2. Enable SNMP read from FortiSIEM.

Sample Events

FortiSIEM generated performance monitoring events:

```
[PH_DEV_MON_FORTIAP_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortinet.cpp,
[lineNumber]=688,[hostName]=FAP320C-default,[hostIpAddr]=,[sysUpTime]=7588440,
[wtpDaemonUpTime]=7588440,[wtpSessionUpTime]=63039960,[numWlanClient]=0,
[ftntWtpSessionStatus]=55038712,[sentBitsPerSec]=0.000000,[recvBitsPerSec]=0.000000,
[pollIntv]=180,[phLogDetail]=

[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortinet.cpp,
[lineNumber]=698,[cpuName]=FAP320C-default_WTP_CPU,[hostName]=FAP320C-default,
[hostIpAddr]=,[cpuUtil]=0.000000,[pollIntv]=0,[phLogDetail]=
[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortinet.cpp,
[lineNumber]=707,[memName]=FAP320C-default_WTP_MEM,[hostName]=FAP320C-default,
[hostIpAddr]=,[memUtil]=34,[totalMemKB]= 254256 ,[freeMemKB]=254256,[usedMemKB]=0,
[phLogDetail]=
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiAP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

FortiWLC

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials
- Sample Events

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller – Name, OS, Serial Number, Interfaces, Associated Access Points – name, OS, Interfaces	Controller – CPU, Memory, Disk, Throughput, QoS statistics, Station count	Performance and Availability Monitoring
Syslog		Hardware/Software errors, failures, logons, license expiry, Access Point Association / Disassociation	Security Monitoring and log analysis

Event Types

In **ADMIN > Device Support > Event Types**, search for "FortiWLC" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

To configure syslog for FortiWLC, see the following knowledgebase article How to send station-log messages from FortiWLC to external sys-log server.

Configure FortiWLC to:

1. Send Syslog to FortiSIEM.
2. Enable SNMP read from FortiSIEM.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Fortinet FortiWLC
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Sample Events

FortiSIEM generated performance monitoring events:

```
[PH_DEV_MON_SYS_CPU_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=281,[cpuName]=CPU,[hostName]=FWLCDemo,[hostIpAddr]=172.30.72.40,
[cpuUtil]=2.000000,[sysCpuUtil]=0.000000,[userCpuUtil]=2.000000,[waitCpuUtil]=98.000000,
[pollIntv]=176,[phLogDetail]=
[PH_DEV_MON_SYS_DISK_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=286,[diskName]=Disk,[hostName]=FWLCDemo,[hostIpAddr]=172.30.72.40,
[diskUtil]=65.000000,[totalDiskMB]=1084,[availDiskMB]=367,[pollIntv]=176,[phLogDetail]=

[PH_DEV_MON_SYS_MEM_UTIL]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=284,[memName]=PhysicalMemory,[hostName]=FWLCDemo,[hostIpAddr]=172.30.72.40,
[memUtil]=9.000000,[totalMemKB]=3922244,[freeMemKB]=3538244,[usedMemKB]=384000,
[phLogDetail]=

[PH_DEV_MON_FORTIWLC_SYS_THRUPUT]:[eventSeverity]=PHL_INFO,
[fileName]=deviceFortiWLCWLAN.cpp,[lineNumber]=343,[hostIpAddr]=172.30.72.40,
[pollIntv]=180,[recvBytes]=3940593459,[sentBytes]=4002693999,[recvBitsPerSec]=0.000000,
[sentBitsPerSec]=0.000000,[wlanRecvBytes]=10851874907433110752,
[wlanSentBytes]=9983789733519268498,[wlanRecvBitsPerSec]=0.000000,
[wlanSentBitsPerSec]=0.000000,[phLogDetail]=

[PH_DEV_MON_FORTIWLC_QOS_STAT]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=426,[hostIpAddr]=172.30.72.40,[pollIntv]=176,[qosSessionCount]=1,
[qosH323SessionCount]=2,[qosSipSessionCount]=3,[qosSccpSessionCount]=4,
[qosRejectedSessionCount]=5,[qosRejectedH323SessionCount]=6,
[qosRejectedSipSessionCount]=7,[qosRejectedSccpSessionCount]=8,[qosPendingSessionCount]=9,
[qosH323PendingSessionCount]=10,[qosSipPendingSessionCount]=11,
[qosSccpPendingSessionCount]=12,[qosActiveFlowCount]=13,[qosPendingFlowCount]=14,
[phLogDetail]=

[PH_DEV_MON_FORTIWLC_STATIONS]:[eventSeverity]=PHL_INFO,[fileName]=deviceFortiWLCWLAN.cpp,
[lineNumber]=511,[hostIpAddr]=172.30.72.40,[pollIntv]=176,[station11a]=1,[station11an1]=2,
[station11an2]=3,[station11an3]=4,[station11b]=5,[station11bg]=6,[station11gn1]=7,
[station11gn2]=8,[station11gn3]=9,[stationData]=10,[stationPhone]=11,[stationWired]=12,
[station11ac1]=13,[station11ac2]=14,[station11ac3]=15,[stationUnknown]=16,[phLogDetail]=
```

FortiWLC Syslog

```
Apr 09 15:07:54 172.18.37.203 ALARM: 12708266551 | system | info | ALR | RADIUS SERVER
SWITCHOVER FAILED MAJOR Primary RADIUS Server <172.18.1.3> failed. No valid Secondary
RADIUS Server present. Switchover FAILED for Profile <4089wpa2>
```

Motorola WiNG WLAN AP

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Syslog		All system logs: User authentication, Admin authentication, WLAN attacks, Wireless link health	Availability, Security and Compliance

Event Types

Over 127 event types - In **ADMIN > Device Support > Event Types**, search for "Motorola-WiNG" to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure devices to send syslog to FortiSIEM - make sure that the version matches the format below.

```
2015-11-11T13:00:16.720960-06:00 co-ap01 %DOT11-5-EAP_FAILED: Client 'FC-C2-DE-B1-43-81'
failed 802.1x/EAP authentication on wlan 'OFFICE-WAREHOUSE-RADIUS-WLAN' radio 'co-ap01:R1'

2015-11-11T12:52:20.437659-06:00 us600001 %SMRT-5-COV_HOLE_RECOVERY_DONE: Radio us-ap10:R2
power changed from 19 to 14
```

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Motorola WiNG WLAN AP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Ruckus Wireless LAN

- What is Discovered and Monitored
- Event Types
- Rules
- Reports
- Configuration
- Settings for Access Credentials

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
SNMP	Controller host name, Controller hardware model, Controller network interfaces, Associated WLAN Access Points	Controller Uptime, Controller Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths), Controller WLAN Statistics, Access Point Statistics, SSID performance Stats	Availability and Performance Monitoring

Event Types

- PH_DEV_MON_RUCKUS_CONTROLLER_STAT

```
[PH_DEV_MON_RUCKUS_CONTROLLER_STAT]:[eventSeverity]=PHL_INFO,
[fileName]=deviceRuckusWLAN.cpp,[lineNumber]=555,[hostName]=guest-zd-01,
[hostIpAddr]=172.17.0.250,[numAp]=41,[numWlanClient]=121,[newRogueAP]=0,
[knownRogueAP]=0,[wlanSentBytes]=0,[wlanRecvBytes]=0,[wlanSentBitsPerSec]=0.000000,
[wlanRecvBitsPerSec]=0.000000,[lanSentBytes]=166848,[lanRecvBytes]=154704,
[lanSentBitsPerSec]=7584.000000,[lanSentBitsPerSec]=7032.000000,[phLogDetail]=
```

- PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT

```
[PH_DEV_MON_RUCKUS_ACCESS_POINT_STAT]:[eventSeverity]=PHL_INFO,
[fileName]=deviceRuckusWLAN.cpp,[lineNumber]=470,[hostName]=AP-10.20.30.3,
[hostIpAddr]=10.20.30.3,[description]=,[numRadio]=0,[numWlanClient]=0,[knownRogueAP]=0,
[connMode]=layer3,[firstJoinTime]=140467251729776,[lastBootTime]=140467251729776,
[lastUpgradeTime]=140467251729776,[sentBytes]=0,[recvBytes]=0,[sentBitsPerSec]=0.000000,
[recvBitsPerSec]=0.000000,[phLogDetail]=
```

- PH_DEV_MON_RUCKUS_SSID_PERF

```
[PH_DEV_MON_RUCKUS_SSID_PERF]:[eventSeverity]=PHL_INFO,[fileName]=deviceRuckusWLAN.cpp,
[lineNumber]=807,[hostName]=c1cs-guestpoint-zd-01,[hostIpAddr]=172.17.0.250,
[wlanSsid]=GuestPoint,[description]=Welcome SSID for not yet authorized APs.,
[wlanName]=Welcome SSID,[authenMethod]=open,[encryptAlgo]=none,[isGuest]=1,
[srcVLAN]=598,[sentBytes]=0,[recvBytes]=0,[sentBitsPerSec]=0.000000,
[recvBitsPerSec]=0.000000,[authSuccess]=0,[authFailure]=0,[assocSuccess]=0,
[assocFailure]=0,[assocDeny]=0,[disassocAbnormal]=0,[disassocLeave]=0,[disassocMisc]=0,
[phLogDetail]=
```

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

Configure the Controller so that FortiSIEM can connect to via SNMP.

Settings for Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device.

Setting	Value
Name	<set name>
Device Type	Ruckus SmartOS WLAN AP
Access Protocol	See Access Credentials
Port	See Access Credentials
Password config	See Password Configuration

Using Virtual IPs to Access Devices in Clustered Environments

FortiSIEM communicates to devices and applications using multiple protocols. In many instances, access credentials for discovery protocols such as SNMP and WMI must be associated to the real IP address (assigned to a network interface) of the device, while application performance or synthetic transaction monitoring protocols (such as JDBC) will need the Virtual IP (VIP) assigned to the cluster. Since FortiSIEM uses a single access IP to communicate to a device, you must create an address translation for the Virtual IPs.

1. Log into your FortiSIEM virtual appliance as `root`.
2. Update the mapping in your IP table to map the IP address used in setting up your access credentials to the virtual IP.

   ```
   iptables -t nat -A OUTPUT -p tcp --destination <access-ip> --dport <destPort> -j DNAT --to-destination <virtual-ip>:<destPort>'
   ```

As an example, suppose an Oracle database server is running on a server with a network address of `10.1.1.1`, which is in a cluster with a VIP of `192.168.1.1`. The port used to communicate with Oracle over JDBC is 1521. In this case, the update command would be:

```
iptables -t nat -A OUTPUT -p tcp --destination 10.1.1.1 --dport 1521 -j DNAT --to-destination 192.168.1.1:1521
```

Syslog over TLS

To receive syslog over TLS, a port must be enabled and certificates must be defined. The following configurations are already added to `phoenix_config.txt` in Super/Worker and Collector nodes.

FortiSIEM 5.x:

```
listen_tls_port_list=6514

tls_certificate_file=/etc/pki/tls/certs/tls_self_signed.crt

tls_key_file=/etc/pki/tls/private/tls_self_signed.key
```

FortiSIEM 6.x:

```
listen_tls_port_list=6514

tls_certificate_file=/etc/pki/tls/certs/localhost.crt

tls_key_file=/etc/pki/tls/private/localhost.key
```

Note: The syslog over TLS client must be configured to communicate properly with FortiSIEM.

Common Reasons to use Syslog over TLS

- You are trying to send syslog across an unprotected medium such as the public internet.
- A SaaS product on the Public internet supports sending Syslog over TLS.

Common Integrations that require Syslog over TLS

- SentinelOne Portal Syslog Integration
- Cortex XDR Syslog Integration

Prerequisites

- If using Syslog over TLS over the public internet or with a public DNS, a public IP or port forwarding is required.
- Add a whitelist to restrict all traffic only from the senders source IPs if possible. Certain SaaS products may publish an IP whitelist, while for others, it may not be possible.

How to Generate a Public SSL/TLS Certificate

Take the following steps:

1. Generate a SSL/TLS certificate using a public certificate. A public certificate can be signed by a public certificate authority (CA) such as DigiCert, or GoDaddy.
2. Run the following command on your collector to generate a CSR (Certificate Signing Request)
   ```
   cd /tmp
   openssl req -new -newkey rsa:4096 -nodes -keyout /etc/pki/tls/private/tls-collector1.key -out tls-collector1.csr
   ```
3. Take the following actions when prompted.
   a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
   b. Enter your State or Province. For example, California would be "CA".
   c. Enter your Locality. For example, a city would be "Sunnyvale".
   d. Enter your desired org name. For example, "Fortinet".
   e. Enter Unit Name, which is optional. For example, "IT".
   f. Enter Common Name. It must match the FQDN of collector. For example, "collector1.myorg.fortinet.com".
   g. Email Address. This can be left blank. Hit "enter" to continue.
   h. If prompted for a challenge password, hit "enter" to leave blank and continue.
   i. Hit enter again to confirm.
      A Certificate Signing Request is created in `/tmp/tls-collector1.csr`.
4. Using WinScp or another SCP utility, download this CSR file to your desktop.
5. Go to your preferred public CA, and upload this CSR when prompted to generate a new SSL certificate file.

   When you have your new Certificate ZIP file, it will normally contain 2-3 files.
6. WinSCP zip file to `/tmp` of the Collector.
7. Unzip the file if needed, by using the following command.
   ```
   unzip <filename>.zip
   ```
   The .crt file is your certificate, and is usually a concatenation of all chain certificates.
8. Rename the cert files if needed using similar commands here.
   ```
   cd /tmp
   mv 11111111.crt tls-collector1.crt
   ```
9. Copy the cert to the correct folder using the following command.
   ```
   cp tls-collector1.crt /etc/pki/tls/certs/tls-collector1.crt
   ```
10. Set permissions using the following command.
    ```
    chmod 644 /etc/pki/tls/certs/tls-collector1.crt
    chmod 640 /etc/pki/tls/private/tls-collector1.key
    chown root:admin /etc/pki/tls/private/tls-collector1.key
    ```
11. On the Collector, update the `/opt/phoenix/config/phoenix_config.txt` file to reference the new tls cert using the following command.
    ```
    vi /opt/phoenix/config/phoenix_config.txt
    ```
12. Locate the following lines in your `phoenix_config.txt` file.
    ```
    listen_tls_port_list=6514
    tls_certificate_file=/etc/pki/tls/certs/localhost.crt
    tls_key_file=/etc/pki/tls/private/localhost.key
    ```
    and replace the cert and key file with the following:
    ```
    listen_tls_port_list=6514
    tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt
    tls_key_file=/etc/pki/tls/private/tls-collector1.key
    ```

13. Save the file, and as root, restart phParser using the following command.

    ```
    killall -9 phParser
    ```

How to Generate a Self Signed SSL/TLS Certificate

Take the following steps:

1. On the Collector, run the following commands as root.

   ```
   cd /tmp
   openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 -keyout
   /etc/pki/tls/private/tls-collector1.key -out /etc/pki/tls/certs/tls-collector1.crt
   ```

2. Take the following actions when prompted.
   a. When Prompted for Country Name, enter your Country Abbreviation. For example, the United States is "US".
   b. Enter your State or Province. For example, California would be "CA".
   c. Enter your Locality. For example, a city would be "Sunnyvale".
   d. Enter your desired org name. For example, "Fortinet".
   e. Enter Unit Name, which is optional. For example, "IT".
   f. Enter Common Name. It must match the FQDN of collector. For example, "collector1.myorg.fortinet.com".
   g. Email Address. This can be left blank. Hit "enter" to continue.
   h. If prompted for a challenge password, hit "enter" to leave blank and continue.
   i. Hit enter again to confirm.
3. Set the appropriate permissions for the private key and certificate generated, by running the following commands.

   ```
   chmod 640 /etc/pki/tls/private/tls-collector1.key
   chown root:admin /etc/pki/tls/private/tls-collector1.key
   chmod 644 /etc/pki/tls/certs/tls-collector1.crt
   ```

4. On the collector, update the `/opt/phoenix/config/phoenix_config.txt` file to reference the new tls certificate by editing the file, running the following command.

   ```
   vi /opt/phoenix/config/phoenix_config.txt
   ```

5. Find the following lines in the file.

   ```
   listen_tls_port_list=6514
   tls_certificate_file=/etc/pki/tls/certs/localhost.crt
   tls_key_file=/etc/pki/tls/private/localhost.key
   ```

   and replace the cert and key file with the following:

   ```
   listen_tls_port_list=6514
   tls_certificate_file=/etc/pki/tls/certs/tls-collector1.crt
   tls_key_file=/etc/pki/tls/private/tls-collector1.key
   ```

6. Save the file, and as root, restart phParser using the following command.

   ```
   killall -9 phParser
   ```

7. Make a copy of the certificate file to `/tmp`, and using WinSCP or another SCP utility, download the Collector Certificate file. For example, you may run the following command.

   ```
   cp /etc/pki/tls/certs/tls-collector1.crt /tmp
   ```

8. Download `/tmp/tls-collector1.crt` to your desktop.
   Note: You only need the Certificate file and not the private key. The private key will never leave the collector.

SNMP V3 Traps

Take the following steps to enable FortiSIEM to receive SNMP V3 traps, which require credentials.

1. Configure the external device (e.g. FortiGate Firewall) to send SNMP V3 traps to the desired FortiSIEM node (typically a Collector). Note down the Authentication and Encryption protocols and passwords. This information is needed for FortiSIEM configuration in step 5. Make sure the external device is sending traps to the FortiSIEM node.
2. SSH as root to the FortiSIEM node that is going to receive the SNMP V3 trap.
3. Stop `phParser` process, by running the following command.
   ```
   phtools --stop phParser
   ```
4. Get the external device's SNMP engine ID, by taking the following steps:
   a. Run the following command.
   ```
   snmptrapd -f -Dlcd_set_enginetime -Lo
   ```
   b. Grab the engine ID from the output. The following example shows that the engine ID is 0x800030440430313530 (in hex format).
   ```
   [root@FSM-MYCENTOS8 ~]# snmptrapd -f -Dlcd_set_enginetime -Lo
   registered debug token lcd_set_enginetime, 1
   Log handling defined - disabling stderr
   lcd_set_enginetime: engineID 80 00 30 44 04 30 31 35 30 : boots=0, time=0
   lcd_set_enginetime: engineID 80 00 30 44 04 30 31 35 30 : boots=1612992361,
   time=28525184
   ```
5. Update the `/etc/snmp/snmptrapd.conf` file by adding the authentication and encryption credentials for the external device's engine ID in hex format.
   ```
   createUser -e <engineId> <user> <authProto> <snmpv3authPwd> <encryptProto>
   <snmpv3encryptPwd>
   ```
   For example:
   ```
   createUser -e 0x800030440430313530 trapuser SHA snmpv3authpass AES
   snmpv3encryptpass
   ```
   Note: You can have multiple entries, but keep in mind that you must have one for each engine ID if multiple devices are sending traps to this FortiSIEM node.
6. Start `phParser` process by running the following command.
   ```
   phtools --start phParser
   ```
7. Run `phstatus` to make sure all processes are up.

   You should now be receiving SNMP3 V3 Traps. You can go to **ANALYTICS** and run historical searches for the external device’s reporting IP.

Appendix

CyberArk to FortiSIEM Log Converter XSL

```
<?xml version="1.0" ?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:import href='./Syslog/RFC5424Changes.xsl'/>
  <xsl:output method="text" version="1.0" encoding="UTF-8" />
  <xsl:template match="/">
  <xsl:apply-imports />
  <xsl:for-each select="syslog/audit_record">
    <xsl:text>CYBERARK: Product="</xsl:text>
      <xsl:value-of select="Product" />
    <xsl:text>"</xsl:text>
    <xsl:text>;Version="</xsl:text>
         <xsl:value-of select="Version" />
    <xsl:text>"</xsl:text>
    <xsl:text>;Hostname="</xsl:text>
         <xsl:value-of select="Hostname" />
    <xsl:text>"</xsl:text>
    <xsl:text>;MessageID="</xsl:text>
      <xsl:value-of select="MessageID" />
    <xsl:text>"</xsl:text>
    <xsl:text>;Message="</xsl:text>
      <xsl:value-of select="Message" />
    <xsl:text>"</xsl:text>
    <xsl:choose>
      <xsl:when test="Desc!=''">
        <xsl:text>;Desc="</xsl:text>
             <xsl:value-of select="Desc" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
      <xsl:when test="Action!=''">
        <xsl:text>;Action="</xsl:text>
             <xsl:value-of select="Action" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
      <xsl:when test="Location!=''">
        <xsl:text>;Location="</xsl:text>
             <xsl:value-of select="Location" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:text>;Issuer="</xsl:text>
      <xsl:value-of select="Issuer" />
    <xsl:text>"</xsl:text>
    <xsl:choose>
      <xsl:when test="Station!=''">
        <xsl:text>;Station="</xsl:text>
          <xsl:value-of select="Station" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
      <xsl:when test="File!=''">
        <xsl:text>;File="</xsl:text>
          <xsl:value-of select="File" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
      <xsl:when test="Safe!=''">
        <xsl:text>;Safe="</xsl:text>
          <xsl:value-of select="Safe" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
      <xsl:when test="Category!=''">
        <xsl:text>;Category="</xsl:text>
          <xsl:value-of select="Category" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
      <xsl:when test="RequestId!=''">
        <xsl:text>;RequestId="</xsl:text>
          <xsl:value-of select="RequestId" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
      <xsl:when test="Reason!=''">
        <xsl:text>;Reason="</xsl:text>
          <xsl:value-of select="Reason" />
        <xsl:text>"</xsl:text>
      </xsl:when>
    </xsl:choose>
    <xsl:choose>
```

```
        <xsl:when test="SeverityCategory!=''">
          <xsl:text>;Severity="</xsl:text>
            <xsl:value-of select="Severity" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="GatewayStation!=''">
          <xsl:text>;GatewayStation="</xsl:text>
            <xsl:value-of select="GatewayStation" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="SourceUser!=''">
          <xsl:text>;SourceUser="</xsl:text>
            <xsl:value-of select="SourceUser" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="TargetUser!=''">
          <xsl:text>;TargetUser="</xsl:text>
            <xsl:value-of select="TargetUser" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="TicketID!=''">
          <xsl:text>;TicketID="</xsl:text>
            <xsl:value-of select="TicketID" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="LogonDomain!=''">
          <xsl:text>;LogonDomain="</xsl:text>
            <xsl:for-each select="CAProperties/CAProperty">
              <xsl:if test="@Name='LogonDomain'">
                <xsl:value-of select="@Value" />
              </xsl:if>
            </xsl:for-each>
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="Address!=''">
          <xsl:text>;Address="</xsl:text>
            <xsl:for-each select="CAProperties/CAProperty">
              <xsl:if test="@Name='Address'">
                <xsl:value-of select="@Value" />
              </xsl:if>
            </xsl:for-each>
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="CPMStatus!=''">
          <xsl:text>;CPMStatus="</xsl:text>
            <xsl:for-each select="CAProperties/CAProperty">
              <xsl:if test="@Name='CPMStatus'">
                <xsl:value-of select="@Value" />
              </xsl:if>
            </xsl:for-each>
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="Database!=''">
          <xsl:text>;Database="</xsl:text>
            <xsl:for-each select="CAProperties/CAProperty">
              <xsl:if test="@Name='Database'">
                <xsl:value-of select="@Value" />
              </xsl:if>
            </xsl:for-each>
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="DeviceType!=''">
          <xsl:text>;DeviceType="</xsl:text>
            <xsl:for-each select="CAProperties/CAProperty">
              <xsl:if test="@Name='DeviceType'">
                <xsl:value-of select="@Value" />
              </xsl:if>
            </xsl:for-each>
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      <xsl:choose>
        <xsl:when test="ExtraDetails!=''">
          <xsl:text>;ExtraDetails="</xsl:text>
            <xsl:value-of select="ExtraDetails" />
          <xsl:text>"</xsl:text>
        </xsl:when>
      </xsl:choose>
      </xsl:for-each>
    <xsl:text>&#13;&#10;</xsl:text>
```

```
    </xsl:template>
  </xsl:stylesheet>
```

Access Credentials

- SNMP Access Credentials
- SSH Access Credentials
- Telnet Access Credentials
- HTTPS Access Credentials
- Password Configuration
    - Manual Password Configuration
    - CyberArk SDK Password Configuration
    - CyberArk REST API Password Configuration
    - RAX_CustomerService Password Configuration
    - RAX_Janus Password Configuration
    - RAX_MSCloud Password Configuration

SNMP Access Credentials

Set these **Access Method Definition** values to allow FortiSIEM to communicate with your device over SNMP.

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	SNMP
Community String	<your own>

SSH Access Credentials

These are the generic settings for providing SSH access to your device from FortiSIEM.

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	SSH
Port	22
Password Config	See Password Configuration
User Name	A user who has permission to access the device over SSH

Setting	Value
Password	The password associated with the user
Super Password	Enter the super password for the system, if required
Organization	Select an organization from the drop-down list

Telnet Access Credentials

These are the generic settings for providing Telnet access to your device from FortiSIEM

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	Telnet
Port	23
Password Config	See Password Configuration
User Name	A user who has permission to access the device over Telnet
Password	The password associated with the user
Super Password	Enter the super password for the system, if required
Organization	Select an organization from the drop-down list

HTTPS Access Credentials

Setting	Value
Name	<set name>
Device Type	<device>
Access Protocol	HTTPS
Port	443
URI	URI address
Password Config	See Password Configuration
User Name	A user who has permission to access the device over HTTPS
Password	The password associated with the user
Organization	Select an organization from the drop-down list

Password Configuration

- Manual Password Configuration
- CyberArk SDK Password Configuration
- CyberArk REST API Password Configuration
- RAX_CustomerService Password Configuration
- RAX_Janus Password Configuration
- RAX_MSCloud Password Configuration

Manual Password Configuration

Settings	Description
User Name	The user name for this account
Password	The password for this account
Super Password	The super password for this account
Organization	Select an organization from the drop-down list

CyberArk SDK Password Configuration

Settings	Description
App ID	Application ID (AccelOps)
Safe	Safe value
Folder	Folder location (Root)
Object	Object name
User Name	User name
Platform (Policy ID)	Policy ID
Database	Database name
Include Address for Query	
Organization	Select an organization from the drop-down list
Description	Description or comments about the credentials

CyberArk REST API Password Configuration

Settings	Description
Endpoint	The endpoint location of the CyberArk device
Root CA	The root certificate authority
SSL Certificate	Secure sockets layer certificate for authentication
SSL Key File	Secure sockets layer key file for encryption and decryption
App ID	Application ID (AccelOps)
Safe	Safe value
Folder	Folder location (Root)
Object	Object name
User Name	User name
Platform (Policy ID)	Policy ID
Database	Database name
Include Address for Query	
Session Token	Session ID used to identify a session
Organization	Select an organization from the drop-down list
Description	Description or comments about the credentials

RAX_CustomerService Password Configuration

Settings	Description
AWS Account Number	Enter the account number.
Azure Subscription ID	Enter the subscription ID.

RAX_Janus Password Configuration

Select RAX_Janus as the Password Config. Supply a Session ID if required.

RAX_MSCloud Password Configuration

Settings	Description
Azure Subscription ID	Enter the subscription ID.

FORTINET®

www.fortinet.com