FortiSIEM External Systems Configuration Guide

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, Sep 27, 2017

FortiSIEM 4.9.0 External Systems Configuration Guide

TABLE OF CONTENTS

Change Log **8**
Configuring External Systems for Discovery and Monitoring **9**
Ports Used by FortiSIEM for Discovery and Monitoring 10
Supported Devices and Applications by Vendor 12
FortiSIEM Windows Agents 33
Windows DFS logs 41
Applications 45
Application Server 46
Authentication Server Configuration 77
Database Server Configuration 95
DHCP and DNS Server Configuration 130
Directory Server Configuration 152
Document Management Server Configuration 157
Mail Server Configuration 161
Management Server/Appliance Configuration 169
Remote Desktop Configuration 175
Unified Communication Server Configuration 180
Web Server Configuration 195
Blade Servers 215
Cisco UCS Server Configuration 216
HP BladeSystem Configuration 221
Cloud Applications 222
AWS Access Key IAM Permissions and IAM Policies 223
AWS CloudTrail API Configuration 225
AWS EC2 CloudWatch API Configuration 229
AWS RDS Configuration 231
Box.com Configuration 233
Cisco FireAMP Cloud Configuration 236
Google Apps Audit Configuration 238
Microsoft Azure AuditTrail Configuration 241
Microsoft Office365 Audit Configuration 243
Okta Configuration 249
Salesforce CRM Audit Configuration 250
Console Access Devices 252
Lantronix SLC Console Manager Configuration 252
End point Security Software 253
Bit9 Security Platform Configuration 254

Cisco Security Agent (CSA) Configuration 256
ESET NOD32 Anti-Virus Configuration 259
FortiClient 260
MalwareBytes Configuration 262
McAfee ePolicy Orchestrator (ePO) Configuration 263
Sophos Endpoint Security and Control Configuration 267
Symantec Endpoint Protection Configuration 269
Trend Micro Intrusion Defense Firewall (IDF) Configuration 272
Trend Micro OfficeScan Configuration 273
Environmental Sensors 274
APC Netbotz Environmental Monitor Configuration 275
APC UPS Configuration 278
Generic UPS Configuration 280
Liebert FPC Configuration 282
Liebert HVAC Configuration 284
Liebert UPS Configuration 286
Firewalls 288
Check Point FireWall-1 289
Check Point Provider-1 Firewall 292
Check Point VSX Firewall Configuration 304
Cisco Adaptive Security Appliance (ASA) Configuration 307
Dell SonicWALL Firewall Configuration 313
Fortinet FortiGate Firewall Configuration 315
Juniper Networks SSG Firewall Configuration 319
McAfee Firewall Enterprise (Sidewinder) Configuration 323
Palo Alto Firewall Configuration 324
Sophos UTM Configuration 327
WatchGuard Firebox Firewall Configuration 329
Load Balancers and Application Firewalls 331
Brocade ServerIron ADX Configuration 332
Citrix Netscaler Application Delivery Controller (ADC) Configuration 334
F5 Networks Application Security Manager 336
F5 Networks Local Traffic Manager Configuration 338
F5 Networks Web Accelerator 341
Qualys Web Application Firewall 342
Network Compliance Management Applications 344
Cisco Network Compliance Manager Configuration 344
Intrusion Protection Systems (IPS) 346
AirTight Networks SpectraGuard 347
Cisco FireSIGHT 348

Cisco Intrusion Protection System Configuration 352
Cylance Protect Endpoint Protection 354
Cyphort Cortex Endpoint Protection 355
FireEye Malware Protection System (MPS) 356
FortiDDoS 357
Fortinet FortiSandbox Configuration 358
IBM Internet Security Series Proventia Configuration 360
Juniper DDoS Secure Configuration 363
Juniper Networks IDP Series Configuration 364
McAfee IntruShield Configuration 365
McAfee Stonesoft IPS 367
Motorola AirDefense Configuration 368
Snort Intrusion Protection System Configuration 369
Sourcefire 3D and Defense Center Configuration 374
TippingPoint Intrusion Protection System Configuration 376
Routers and Switches 379
Alcatel TiMOS and AOS Switch Configuration 380
Arista Router and Switch Configuration 382
Brocade NetIron CER Routers 385
Cisco 300 Series Routers 387
Cisco IOS Router and Switch Configuration 389
Cisco Meraki Cloud Controller and Network Devices Configuration 402
Cisco NX-OS Router and Switch Configuration 404
Cisco ONS Configuration 410
Dell Force10 Router and Switch Configuration 412
Dell NSeries Switch Configuration 415
Dell PowerConnect Switch and Router Configuration 417
Foundry Networks IronWare Router and Switch Configuration 420
HP/3Com ComWare Switch Configuration 424
HP ProCurve Switch Configuration 426
HP Value Series (19xx) and HP 3Com (29xx) Switch Configuration 429
Juniper Networks JunOS Switch Configuration 432
Mikrotek Router Configuration 437
Nortel ERS and Passport Switch Configuration 439
Security Gateways 441
Barracuda Networks Spam Firewall Configuration 442
Blue Coat Web Proxy Configuration 444
Cisco IronPort Mail Gateway Configuration 449
Cisco IronPort Web Gateway 451
McAfee Web Gateway Configuration 453

Microsoft ISA Server Configuration 455
Squid Web Proxy Configuration 461
Websense Web Filter Configuration 464
Fortinet FortiMail 466
Fortinet FortiWeb 467
Servers 469
HP UX Server Configuration 470
Settings for Access Credentials 471
IBM AIX Server Configuration 473
IBM OS400 Server Configuration 476
Linux Server Configuration 478
Microsoft Windows Server Configuration 483
Sun Solaris Server Configuration 491
Storage 494
Brocade SAN Switch Configuration 495
Dell Compellant Storage Configuration 497
Dell EqualLogic Storage Configuration 499
EMC Clarion Storage Configuration 502
EMC Isilon Storage Configuration 507
EMC VNX Storage Configuration 509
NetApp Filer Storage Configuration 514
Nimble Storage Configuration 518
Nutanix Storage Configuration 520
Virtualization 525
HyperV 526
VMware ESX Configuration 530
VPN Gateways 532
Cisco VPN 3000 Gateway Configuration 533
Juniper Networks SSL VPN Gateway Configuration 535
Microsoft PPTP VPN Gateway Configuration 537
PulseSecure Configuration 538
Vulnerability Scanners 540
McAfee Foundstone Vulnerability Scanner Configuration 541
Qualys Vulnerability Scanner Configuration 545
Rapid7 NeXpose Vulnerability Scanner Configuration 547
WAN Accelerators 549
Cisco Wide Area Application Server Configuration 550
Riverbed SteelHead WAN Accelerator Configuration 552
Wireless LANs 555
Aruba Networks Wireless LAN Configuration 556

Cisco Wireless LAN Configuration 558
FortiAP 561
FortiWLC 563
Motorola WiNG WLAN AP Configuration 565
Ruckus Wireless LAN Configuration 566
Using Virtual IPs to Access Devices in Clustered Environments 568
Syslog over TLS 569

Change Log

Date	Change Description
2017-15-05	Initial version for release 4.9.0

Configuring External Systems for Discovery and Monitoring

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
- FortiSIEM Windows Agent and Agent Manager
- Applications
- Blade Servers
- Cloud Applications
- Console Access Devices
- End point Security Software
- Environmental Sensors
- Firewalls
- Load Balancers and Application Firewalls
- Network Compliance Management Applications
- Network Intrusion Protection Systems (IPS)
- 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

Ports Used by FortiSIEM for Discovery and Monitoring

These ports are used by FortiSIEM to discover devices, pull metrics and process event logs.

Ports	Services	Super	Worker	Collector
UDP/514	UDP syslog	x	x	x
TCP/1470	TCP syslog	x	x	x
UDP/6514	UDP syslog over TLS	x	x	x
TCP/6514	TCP syslog over TLS	x	x	x
UDP/2055	netflow	x	x	x
TCP/22	ssh	x	x	x
TCP/5480	HTTP Registration			x
ICMP		x	x	x
TCP/21	FTP (Receiving Bluecoat logs via ftp)	x	x	x
TCP/5432	postgresql	x		
UDP/111, TCP/111	NFS portmapper	x	x	
TCP/7900	phMonitor	x	x	
TCP/7914	phParser	x	x	
TCP/7916	phQueryWorker	x	x	
TCP/7918	phQueryMaster	x	x	
TCP/7920	phDataManager	x	x	
TCP/7922	phRuleMaster	x	x	
TCP/7924	phRuleWorker	x	x	
TCP/7926	phAgentManager	x	x	

Ports	Services	Super	Worker	Collector
TCP/7928	phDiscover	x	x	
TCP/7930	phCheckpoint	x	x	
TCP/7932	phReportWorker	x	x	
TCP/7934	phReportMaster	x	x	
TCP/7936	phEventPackager	x	x	
TCP/7938	phIpIdentityMaster	x	x	
TCP/7940	phIpIdentityWorker	x	x	
TCP/110	POP3	x		
TCP/135	WMI	x	x	x
TCP/143	IMAP	x		
UDP/161	SNMP	x	x	x
UDP/162	SNMP TRAP	x	x	x
TCP/389	LDAP	x	x	x
TCP/443	HTTPS	x	x	x
TCP/993	IMAP/SSL	x		
TCP/995	POP/SSL	x		
TCP/1433	JDBC	x	x	x
UDP/8686	JMX	x	x	x
TCP/18184	Checkpoint LEA	x	x	x
TCP/18190	Checkpoint CPMI Port	x	x	x

Supported Devices and Applications by Vendor

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration 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
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 CloudWatch AWS 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 Relational Database Storage (RDS)		CloudWatch API: CPU, Connections, Memory, Swap, Read/Write Latency and Ops			AWS EBS and RDS
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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	
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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
Checkpoint	FireWall-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, NGX, and R75	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	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	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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
Cisco	FWSM	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	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	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	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, power supply unit, fan unit	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	Configuration Change monitoring	Details
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 Telepresence 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 Telepresence 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
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
Cisco	Sourcefire 3D and Defense Center	SNMP: OS, Hardware				Sourcefire 3D and Defense Center
Cisco	FireSIGHT Console			eStreamer SDK: Intrusion events, Malware events, File events, Discovery events, User activity events, Impact flag events		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
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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
Cylance	Cylance Protect Endpoint Protection			Syslog: Endpoint protection alerts		Cylance Protect
Cyphort	Cyphort Cortex Endpoint Protection			Syslog: Endpoint protection alerts		Cyphort Cortex
Dell	SonicWall Firewall	SNMP: OS, Hardware	SNMP: CPU, Memory, Interface utilization, Firewall session count	Syslog: Firewall log analysis (over 1000 event types)	Currently not natively supported	Dell SonicWALL
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 Compellant
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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 Clarion
EMC	VNX 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			EMC VNX

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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			EMC Isilon
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		
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	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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
Fortinet	FortiCient	Discovery via LOG		Syslog: Traffic logs, Event logs		FortiCient
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		FortiWLC
Fortinet	FortiAP	Access point – Name, OS, Interfaces, Controller (FortiGate)	FortiAP CPU, Memory, Clients, Sent/Received traffic	Wireless events via FortiGate		FortiAP
Fortinet	FortiManager	SNMP: Host name, Hardware model, Network interfaces, Operating system version	SNMP: Uptime, CPU and Memory utilization, Network Interface metrics			FortiManager
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
FreeBSD						
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
HP	HP Hardware on Intel-based Servers	SNMP: hardware model, hardware serial, hardware components (fan, power supply, battery, raid, disk, memory)	SNMP: hardware status	SNMP Trap: Over 100 traps covering hardware issues		
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
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
ISC	Bind DNS			Syslog: DNS logs - name resolution activity - success and failures		ISC BIND DNS
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	Steelbelted 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 - Over 5500 IPS Alert types parsed		Juniper Networks IDP Series
Juniper	DDoS Secure			Syslog - DDoS Alerts		Juniper DDoS
Lantronix	SLC Console Manager			Syslog - Admin access, Updates, Commands run		Lantronix SLC Console Manager

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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
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, Running Processes, Services, Installed Patches	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 logs	SNMP: Installed Software Change; FortiSIEM Windows Agent: Installed Software Change, Registry Change; FortiSIEM Windows Agent: File Integrity Monitoring	Microsoft Windows Servers
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)

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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	SQL Server - 2005, 2008, 2008R2, 2012, 2014	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	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	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	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	HyperV Hypervisor		Powershell over winexe: Guest/Host CPU usage, Memory usage, Page fault, Disk Latency, Network usage ;			HyperV

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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	Exchange Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage; WMI: Exchange performance metrics, Exchange error metrics, Exchange mailbox metrics, Exchange SMTP metrics, Exchange ESE Database, Exchange Database Instances, Exchange Mail Submission Metrics, Exchange Store Interface Metrics etc			Microsoft Exchange
Microsoft	ISA Server	SNMP: Running Processes	SNMP or WMI: Process level resource usage	FortiSIEM Windows Agent (HTTPS): W3C Access logs - Per Connection - Sent Bytes, Received Bytes, Duration; Snare Agent (syslog): W3C Access logs Correlog Agent (syslog): W3C Access logs		Microsoft ISA 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 - successful and failed		Microsoft PPTP
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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
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
Nessus	Vulnerability Scanner			Nessus 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		Nessus Vulnerability Scanner
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
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
Nutanix	Controller VM	SNMP: Host name, OS, Hardware model, Serial number, Network interfaces, Physical Disks, Components	SNMP: Uptime CPU/memory utilization, Network Interface metrics/errors, Disk Status, Cluster Status, Service Status, Storage Pool Info, Container Info			Nutanix
Okta.com	SSO	Okta API: Users		Okta API: Over 90 event types covering user activity in Okta website		Okta Configuration
OpenLDAP	OpenLDAP	LDAP: Users				
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, table space free space etc; JDBC: Database audit trail: Database log on, Database/Table CREATE/DELETE/MODIFY operations			MySQL Server
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

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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
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
PulseSecure	PulseSecure VPN			Syslog: VPN events, Traffic events, Admin events		PulseSecure
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
Rapid7	NeXpose Vulnerability Scanner			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
Riverbed	Steelhead WAN Accelerators	SNMP: Host name, Software version, Hardware model, Network interfaces	SNMP: Uptime, CPU / Memory / Network Interface / Disk space metrics, Process cpu/memory 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	SNMP Trap: About 115 event types covering software errors, hardware errors, admin login, performance issues - cpu, memory, peer latency issues ; Netflow: Connection statistics		Riverbed SteelHead WAN Accelerator

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
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 WLAN Access Points	SNMP: Controller Uptime, Controller Network Interface metrics, Controller WLAN Statistics, Access Point Statistics, SSID performance Stats			Ruckus WLAN
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	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
Symantec	Symantec Endpoint Protection			Syslog: Over 5000 event types covering end point protection events - malware/spyware/adware, malicious events		Symantec Endpoint Protection

Vendor	Model	Discovery Overview	Performance Monitoring Overview	Log Analysis Overview	Configuration Change monitoring	Details
TrendMicro	Office scan			SNMP Trap: Over 30 event types covering end point protection events - malware/spyware/adware, malicious events		Trend Micro OfficeScan
TrendMicro	Intrusion Defense Firewall (IDF)			Syslog: Over 10 event types covering end point firewall events		Trend Micro IDF
TrendMicro	Deep Security Manager			Syslog: Over 10 event types covering end point protection events		
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, 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

FortiSIEM Windows Agents

This section describes how to setup FortiSIEM Windows Agent and Agent Manager as part of FortiSIEM infrastructure.

- Procedure
- Sample logs generated by FortiSIEM Windows Agents

Procedure

Configure FortiSIEM Supervisor

1. Go to **Admin** > **License Management** and make sure that there are entries for Basic and Advanced Windows Agents.
2. Go to **Admin** > **Setup Wizard** and add Agent Managers
    a. Click on **Windows Agents** tab
    b. Click **Add** and enter information for an Windows Agent Manager. This information will be used by the Agent Manager to register to FortiSIEM
        a. Enter **Agent Manager Name**
        b. Enter the number of **Basic Agents** and **Advanced Agents** assigned to this Agent Manager
        c. Enter the **Start Time** and **End Time** for license validity
        d. Choose **Event Upload Destination** - this is where the Agent Manager will upload events to.
            i. Select the Organization (Super for Enterprise version and Specific Organization for the Service Provider version)
            ii. Select one or more Collectors belonging to the selected organization
        e. Click **OK** to Save

Register Windows Agent Manager to FortiSIEM Supervisor

1. Log on to Windows Agent Manager
2. Launch FortiSIEM Windows Agent Manager application
3. Log on to the FortiSIEM Windows Agent Manager application using **User ID** and **Password** created during setup
4. Register the Windows Agent Manager to FortiSIEM
    a. Enter **Supervisor IP/Host**
    b. Enter **Agent Manager Name** - this is defined in Step 2.b.i in **Configure FortiSIEM Supervisor** step
    c. Enter **Organization Name** - this is defined in Step 2.b.iv in **Configure FortiSIEM Supervisor** step
    d. Enter **Organization User** and **Organization Password** as the Organizations credentials defined when the Organization was created in Admin > Setup wizard.
5. Click Register. If registration is successful, then **Windows Agent ManagerDashboard** page is displayed. All the installed agents show up in this page with Current Status as Running.

Configure Windows Agent Manager

Agent to Multiple Templates

Starting Release 2.0, Agents can be associated with multiple monitoring templates.

Agent to Multiple Collectors

Starting Release 2.1, Agents can be associated with one or more collectors. Windows Agent Manager can associate Agents to Collectors. Agents send events to any collector they choose. If a particular collector is not responsive, Agent will send to other available collectors. Before Release 2.1, Agents sent events to Collector(s) via Windows Agent Manager.

1. Go to **Dashboard** and make sure that it displays all Windows Servers with FortiSIEM agents installed.
2. Create a Monitoring Template
    i. Go to **Template Settings**. Click on **+** to expand the options.
    ii. Click **Create Template**.
        a. Enter a template name and description. Click **Settings**.
        b. Specify options for each monitoring category
        c. Associate Windows Computers with proper license and one or more Templates (Starting with release 2.0) and one or more collectors (starting with release 2.1).

Category	Description	Settings
File/Folder Changes	Monitor access and change to files and folders	a. Click **New**. b. Enter the full path of File/Folder to be modified c. Select Include Subfolder(s) if the folders under the main directory needs to be monitored. d. Narrow down the scope by either specify **Include** or **Exclude** files. The chosen files/directories will be displayed (**Note:** To get User information, you have do some special configuration in Windows Agents as defined in Step 2 of Pre-requisites in Installing FortiSIEM Windows Agent)

Category	Description	Settings
Registry Changes	Monitor changes to the root keys of Windows Registry hive	Select the root keys (available keys are `HK_CLASSES_ROOT`, `HKEY_CURRENT_USER`, `HKEY_LOCAL_MACHINE`, `HKEY_USERS`, and `HKEY_CURRENT_CONFIG`) Set the time interval for how often the Agent will check for change. More CPU will be used for shorter time intervals
Installed Software	Monitor software install / uninstall on a Windows server	Select Product Name, Version and Vendor to be included in an event when a change is detected.
Logs	Collect System/Security/Application logs and specific application logs	Check **System** if you want to collect Windows System logs. Specify include/exclude event ids. Check **Security** if you want to collect Windows Security logs. Specify include/exclude event ids. Check **DNS** if you want to collect Windows DNS logs. Specify include/exclude event ids. Check **DFS** if you want to collect Windows DFS logs. Specify include/exclude event ids. Check **Application** if you want to collect Windows Application logs. Specify include/exclude event ids. Check **IIS** if you want to collect Windows IIS logs. Specify include/exclude event ids. Check **DHCP** if you want to collect Windows DHCP logs. Specify include/exclude event ids. Check **User Logs** and specify the file (s) you want to monitored. Any time, the file changes, a log will be generated,

Category	Description	Settings
WMI Classes	Run a WMI command and collect its output	Select Category and then select the class Select WMI Class Attributes Specify how often the command needs to run **Note**: you may need to write a parser in FortiSIEM to get accurate attribute based reporting
Powershell Script	Run Powershell command and send its output	Enter a Powershell script Specify how often the Powershell script needs to run **Note**: you may need to write a parser in FortiSIEM to get accurate attribute based reporting

d. Click **Apply** to save the template
e. Click **Save**

3. Associate Windows Computers with proper license and one or more Templates (Starting with release 2.0) and one or more collectors (starting with release 2.1)
    1. Click **Associate License / Templates.**
    2. Click **Search** to find the list of computers to apply the license/templates to
        a. Choose **Simple** or **Advanced**
        b. For **Simple** mode
            i. Select the field to **Search in.** Possible choices are Computer, OS, License Type, Template Name**.**
            ii. Type in the string to search **for** in the adjacent edit box.
            iii. Click **Find**.
            iv. The list of matched computers will be displayed in the area below the Search box.
            v. Select the Computers to which license/templates would be assigned
                i. Select the header checkbox to select/unselect all
                ii. Individually select/unselect the computers if needed
        1. For **Advanced** mode
            a. For searching by computer names, type the search text next to **Computer**.
            b. For searching by OS names, type the search text next to **OS**.
            c. For searching by **License Types**, select the desired license type from the drop down
            d. For searching by **Template Names**, do one of the following.
                i. For exact template name matches, set **Templates** to '**Specified from**' and select one or more templates from the next drop down and select the operator: AND or OR
                ii. For searching template names, set **Templates** to '**Specified in**' and type the search string

e. Click **Find**. The list of matched computers will be displayed in the area below the Search boxSelect a **Template** for a Computer.
f. Select the Computers to which license/templates would be assigned:
    i. Select the header checkbox to select/unselect all.
    ii. Individually select/unselect the computers if needed.

3. Make sure the list of computers in view are correct for the license/template assignment and are checked.
4. Click **Assign**
    1. **License** Assignment
        - Select **License** Type: Basic or Advanced or None.
        - Click **Assign**.
    2. **Template** Assignment
        - Select **Template(s)** from drop down list.
        - Click **Validate**.
        - Click **Assign**. The display would reflect the assignment.
        - Click **Unassign** to remove the template from the computer. The display would reflect the modification.
    3. **Collector** Assignment
        - Select **Collector** and then choose a set of Collectors from the drop down.
        - Click **Associate** to assign the collectors to the Computers. The display would reflect the assignment.
        - Click **Dissociate** to remove the template from the computer. The display would reflect the modification.
        - Click **Associate remaining** to assign the remaining collectors to the Computers.
5. Click **Close**

License and Template Assignments in Agent Manager via Export/Import

1. Logon to Agent Manager
2. Go to **Dashboard** and make sure that the Agents are showing up
3. Click **Export** - a list of Agents Computer name, Assigned license and Assigned template will be exported to a CSV formatted file named 'ExportedAgentAssociation.csv' in the directory **ProgramData|FortiSIEM|Server.**
4. **Edit the** CSV file to associate the right license type and monitoring template to each computer. Do not add any new computer or edit computer. Every computer known to the Agent Manager will be present in the csv file.
5. Click **Import** and put the CSV file in the Open file Dialog.
6. Once Import finishes, a dialog will tell you the number of records processed and successfully updated.
7. Click **Assign Licenses to Computers** to see the License assignments.
8. Click **Associate Computers with Templates** to see Template assignments.
9. Any warnings during import operations will be recorded in <CSVFilename>-<Date>-<Time>.log file in the directory **ProgramData|FortiSIEM|Server.**

Verify Events in FortiSIEM

1. Log on to FortiSIEM.
2. Go to **Analytics** > **Historical Search.**

3. Select **Filter Criteria**: Structured .
4. Create the following condition: **Raw Event Log** CONTAIN FortiSIEM-WUA. Click **OK.** Note that all event types for all Windows Server generated logs are prefixed by FortiSIEM-WUA.
5. Select the following **Group By**:
   a. Reporting Device Name
   b. Reporting IP
6. Select the following **Display Fields:**
   a. Reporting Device Name
   b. Reporting IP
   c. COUNT(Matched Events)
7. Run the query for last 15 minutes.
8. The Query will return all hosts that reported events in the last 15 minutes.
9. To drill down further, add **Event Type** to both **Group By** and **Display Fields**. Then rerun the query.

Sample logs generated by FortiSIEM Windows Agents

FortiSIEM Windows Agent Manager generates Windows logs in an easy to analyze "attribute=value" style without losing any information.

Windows System logs

```
#Win-System-Service-Control-Manager-7036

Thu May 07 02:13:42 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="System"
[eventSource]="Service Control Manager" [eventId]="7036" [eventType]="Information"
[domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:13:41"
[deviceTime]="May 07 2015 10:13:41"
[msg]="The Skype Updater service entered the running state."
Thu May 07 02:13:48 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="System"
[eventSource]="Service Control Manager" [eventId]="7036" [eventType]="Information"
[domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:13:47"
[deviceTime]="May 07 2015 10:13:47"
[msg]="The Skype Updater service entered the stopped state."
```

Windows Application logs

```
#Win-App-MSExchangeServiceHost-2001
Thu May 07 03:05:42 2015 WIN-2008-249.ersijiu.com 10.1.2.249 FortiSIEM-WUA-WinLog
[monitorStatus]="Success" [eventName]="Application" [eventSource]-
]="MSExchangeServiceHost" [eventId]="2001" [eventType]="Information" [domain]=""
[computer]="WIN-2008-249.ersijiu.com"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 11:05:42"
[deviceTime]="May 07 2015 11:05:42"
[msg]="Loading servicelet module Microsoft.Exchange.OABMaintenanceServicelet.dll"
#MSSQL
#Win-App-MSSQLSERVER-17137
Thu May 07 03:10:16 2015 WIN-2008-249.ersijiu.com 10.1.2.249 FortiSIEM-WUA-WinLog
```

```
[monitorStatus]="Success" [eventName]="Application"
[eventSource]="MSSQLSERVER" [eventId]="17137" [eventType]="Information"
[domain]="" [computer]="WIN-2008-249.ersijiu.com" [user]=""
[userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 11:10:16" [deviceTime]-
]="May 07 2015 11:10:16"
[msg]="Starting up database 'model'."
```

Windows Security logs

```
#Win-Security-4624(Windows logon success)
Thu May 07 02:23:58 2015 WIN-2008-249.ersijiu.com 10.1.2.249 FortiSIEM-WUA-WinLog
[monitorStatus]="Success" [eventName]="Security"
[eventSource]="Microsoft-Windows-Security-Auditing" [eventId]="4624" [eventType]-
]="Audit Success" [domain]=""
[computer]="WIN-2008-249.ersijiu.com" [user]="" [userSID]="" [userSIDAcctType]=""
[eventTime]="May 07 2015 10:23:56"
[deviceTime]="May 07 2015 10:23:56" [msg]="An account was successfully logged on."
[[Subject]][Security ID]="S-1-0-0" [Account Name]=""
[Account Domain]="" [Logon ID]="0x0" [Logon Type]="3" [[New Logon]][Security ID]-
]="S-1-5-21-3459063063-1203930890-2363081030-500"
[Account Name]="Administrator" [Account Domain]="ERSIJIU" [Logon ID]="0xb9bd3"
[Logon GUID]="{00000000-0000-0000-0000-000000000000}"
[[Process Information]][Process ID]="0x0" [Process Name]="" [[Network Inform-
ation]][Workstation Name]="SP171" [Source Network Address]="10.1.2.171"
[Source Port]="52409" [[Detailed Authentication Information]][Logon Pro-
cess]="NtLmSsp" [Authentication Package]="NTLM" [Transited Services]=""
[Package Name (NTLM only)]="NTLM V2" [Key Length]="128" [details]=""
```

Windows DNS logs

```
#DNS Debug Logs
#AO-WUA-DNS-Started
Thu May 07 02:35:43 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DNS [mon-
itorStatus]="Success"
[msg]="5/7/2015 10:34:05 AM 20BC EVENT   The DNS server has started."
#AO-WUA-DNS-ZoneDownloadComplete
Thu May 07 02:35:43 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DNS [mon-
itorStatus]="Success" [msg]="5/7/2015 10:34:05 AM 20BC EVENT
The DNS server has finished the background loading of zones. All zones are now
available for DNS updates and zone
transfers, as allowed by their individual zone configuration."
#AO-WUA-DNS-A-Query-Success
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DNS [mon-
itorStatus]="Success" [msg]="5/7/2015
 10:47:13 AM 5D58 PACKET  0000000002B74600 UDP Rcv 10.1.20.232  0002   Q [0001   D
  NOERROR] A      (8)testyjyj(4)yjyj(3)com(0)"Thu May 07 02:48:25 2015 WIN-2008-
LAW-agent 10.1.2.242 FortiSIEM-WUA-DNS [monitorStatus]="Success" [msg]="5/7/2015
 10:47:13 AM 5D58 PACKET  0000000002B74600 UDP Snd 10.1.20.232     0002 R Q [8085
A DR  NOERROR] A      (8)testyjyj(4)yjyj(3)com(0)"
#AO-WUA-DNS-PTR-Query-Success
Thu May 07 02:48:25 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DNS
```

```
[monitorStatus]="Success" [msg]="5/7/2015
10:47:22 AM 5D58 PACKET  00000000028AB4B0 UDP Rcv 10.1.20.232 0002   Q [0001   D
NOERROR] PTR
(3)223(3)102(3)102(3)102(7)in-addr(4)arpa(0)"Thu May 07 02:48:25 2015 WIN-2008-
LAW-agent 10.1.2.242 FortiSIEM-WUA-DNS [monitorStatus]="Success" [msg]="5/7/2015
10:47:22 AM 5D58 PACKET  00000000028AB4B0 UDP Snd 10.1.20.232     0002 R Q [8085 A
DR  NOERROR] PTR
(3)223(3)102(3)102(3)102(7)in-addr(4)arpa(0)"
#DNS System Logs
#Win-App-DNS-2(DNS Server started)
Thu May 07 02:39:17 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success"
[eventName]="DNS Server" [eventSource]="DNS" [eventId]="2" [eventType]-
]="Information" [domain]="" [computer]="WIN-2008-LAW-agent"
[user]="" [userSID]="" [userSIDAcctType]="" [eventTime]="May 07 2015 10:39:17"
[deviceTime]="May 07 2015 10:39:17"
[msg]="The DNS server has started." #Win-App-DNS-3(DNS Server shutdown)
Thu May 07 02:39:16 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="DNS Server"
[eventSource]="DNS" [eventId]="3" [eventType]="Information" [domain]="" [com-
puter]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 10:39:16" [deviceTime]="May 07 2015
10:39:16" [msg]="The DNS server has shut down.
```

Windows DHCP logs

```
AO-WUA-DHCP-Generic
Thu May 07 05:44:44 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DHCP [mon-
itorStatus]="Success" [ID]="00" [Date]="05/07/15"
[Time]="13:44:08" [Description]="Started" [IP Address]="" [Host Name]="" [MAC
Address]="" [User Name]="" [ TransactionID]="0"
[ QResult]="6" [Probationtime]="" [ CorrelationID]="" [Dhcid.]=""
#AO-WUA-DHCP-IP-ASSIGN
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DHCP [mon-
itorStatus]="Success" [ID]="10" [Date]="05/07/15"
[Time]="13:56:37" [Description]="Assign" [IP Address]="10.1.2.124" [Host Name]-
]="Agent-247.yj" [MAC Address]="000C2922118E"
[User Name]="" [ TransactionID]="2987030242" [ QResult]="0" [Probationtime]="" [
CorrelationID]="" [Dhcid.]=""
#AO-WUA-DHCP-Generic(Release)
Thu May 07 05:56:41 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DHCP [mon-
itorStatus]="Success" [ID]="12" [Date]="05/07/15"
[Time]="13:56:33" [Description]="Release" [IP Address]="10.1.2.124" [Host Name]-
]="Agent-247.yj" [MAC Address]="000C2922118E"
[User Name]="" [ TransactionID]="2179405838" [ QResult]="0" [Probationtime]="" [
CorrelationID]="" [Dhcid.]=""
#AO-WUA-DHCP-IP-LEASE-RENEW
Wed Feb 25 02:53:28 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-DHCP [mon-
itorStatus]="Success" [ID]="11" [Date]="02/25/15"
[Time]="10:53:19" [Description]="Renew" [IP Address]="10.1.2.123" [Host Name]-
]="WIN-2008-249.yj" [MAC Address]="0050568F1B5D"
```

```
[User Name]="" [ TransactionID]="1136957584" [ QResult]="0" [Probationtime]="" [
CorrelationID]="" [Dhcid.]=""
```

Windows IIS logs

```
#AO-WUA-IIS-Web-Request-Success
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-IIS [mon-
itorStatus]="Success" [date]="2015-05-07"
[time]="03:44:28" [s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-ip]-
]="10.1.2.242" [cs-method]="GET"
[cs-uri-stem]="/welcome.png" [cs-uri-query]="-" [s-port]="80" [cs-username]="-"
[c-ip]="10.1.20.232" [cs-version]="HTTP/1.1"
[cs(User-Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+-
like+Gecko)+Chrome/42.0.2311.135+Safari/537.36"
[cs(Cookie)]="-" [cs(Referer)]="http://10.1.2.242/" [cs-host]="10.1.2.242" [sc-
status]="200" [sc-substatus]="0" [sc-win32-status]="0"
[sc-bytes]="185173" [cs-bytes]="324" [time-taken]="78" [site]="Default Web Site"
[format]="W3C"
#AO-WUA-IIS-Web-Client-Error
Thu May 07 03:49:23 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-IIS [mon-
itorStatus]="Success" [date]="2015-05-07" [time]="03:44:37"
[s-sitename]="W3SVC1" [s-computername]="WIN-2008-LAW-AG" [s-ip]="10.1.2.242" [cs-
method]="GET" [cs-uri-stem]="/wrongpage" [cs-uri-query]="-"
[s-port]="80" [cs-username]="-" [c-ip]="10.1.20.232" [cs-version]="HTTP/1.1" [cs
(User-Agent)]="Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+-
like+Gecko)+Chrome/42.0.2311.135+Safari/537.36" [cs(Cookie)]="-" [cs(Referer)]="-"
[cs-host]="10.1.2.242" [sc-status]="404"
[sc-substatus]="0" [sc-win32-status]="2" [sc-bytes]="1382" [cs-bytes]="347" [time-
taken]="0" [site]="Default Web Site" [format]="W3C"
#AO-WUA-IIS-Web-Forbidden-Access-Denied
Thu May 07 03:30:39 2015 WIN-2008-249.ersijiu.com 10.1.2.249 FortiSIEM-WUA-IIS
[monitorStatus]="Success" [date]="2015-05-07" [time]="03:30:15" [s-ip]-
]="10.1.2.249" [cs-method]="POST" [cs-uri-stem]="/AOCACWS/AOCACWS.svc" [cs-uri-
query]="-" [s-port]="80" [cs-username]="-"
[c-ip]="10.1.2.42" [cs(User-Agent)]="-" [sc-status]="403" [sc-substatus]="4" [sc-
win32-status]="5" [time-taken]="1" [site]="Default Web Site"
[format]="W3C"
```

Windows DFS logs

```
#Win-App-DFSR-1002
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1002" [eventType]="Information" [domain]="" [com-
puter]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015
11:01:12" [msg]="The DFS Replication service is starting."#Win-App-DFSR-1004
Thu May 07 03:01:12 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1004" [eventType]="Information" [domain]="" [com-
puter]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:12" [deviceTime]="May 07 2015
```

```
11:01:12" [msg]="The DFS Replication service has started."#Win-App-DFSR-1006
Thu May 07 03:01:10 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1006" [eventType]="Information" [domain]="" [com-
puter]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:10" [deviceTime]="May 07 2015
11:01:10" [msg]="The DFS Replication service is stopping."#Win-App-DFSR-1008
Thu May 07 03:01:11 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WinLog [mon-
itorStatus]="Success" [eventName]="DFS Replication"
[eventSource]="DFSR" [eventId]="1008" [eventType]="Information" [domain]="" [com-
puter]="WIN-2008-LAW-agent" [user]="" [userSID]=""
[userSIDAcctType]="" [eventTime]="May 07 2015 11:01:11" [deviceTime]="May 07 2015
11:01:11" [msg]="The DFS Replication service has stopped."
```

Windows file content monitoring logs

```
#AO-WUA-UserFile
Thu May 07 05:40:08 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-UserFile [mon-
itorStatus]="Success" [fileName]="C:\test\i.txt"
[msg]="another newline adddeddddddd"
```

Windows File integrity monitoring logs

```
#AO-WUA-FileMon-Added
Thu May 07 05:30:59 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-FileMon [mon-
itorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:30:58" [fileName]="C:\\test\\New Text Document.txt"
[osObjAction]="Added" [hashCode]="d41d8cd98f00b204e9800998ecf8427e"
[msg]=""
#AO-WUA-FileMon-Renamed-New-Name
Thu May 07 05:31:02 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-FileMon [mon-
itorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:30:58" [fileName]="C:\\test\\test.txt" [osOb-
jAction]="Renamed [New Name]" [hashCode]="d41d8cd98f00b204e9800998ecf8427e"
[msg]=""
#AO-WUA-FileMon-Renamed-Old-Name
Thu May 07 05:31:02 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-FileMon [mon-
itorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:31:01" [fileName]="C:\\test\\New Text Document.txt"
[osObjAction]="Renamed [Old Name]" [hashCode]=""
[msg]=""
#AO-WUA-FileMon-Modified
Thu May 07 05:31:14 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-FileMon [mon-
itorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:31:13" [fileName]="C:\\test\\test.txt" [osOb-
jAction]="Modified" [hashCode]="23acb5410a432f14b141656c2e70d104"
[msg]=""
#AO-WUA-FileMon-Removed
Thu May 07 05:31:29 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-FileMon [mon-
itorStatus]="Success" [userId]="Administrator"
[eventTime]="May 07 2015 05:31:27" [fileName]="C:\\test\\test.txt" [osOb-
jAction]="Removed" [hashCode]="" [msg]=""
```

Windows Installed Software logs

```
#AO-WUA-InstSw-Added
Thu May 07 05:28:17 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-InstSw [mon-
itorStatus]="Success" [osObjAction]="Added"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVer-
sion]="9.20.00.0"
#AO-WUA-InstSw-Removed
Thu May 07 05:28:30 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-InstSw [mon-
itorStatus]="Success" [osObjAction]="Removed"
[appName]="7-Zip 9.20 (x64 edition)" [vendor]="Igor Pavlov" [appVer-
sion]="9.20.00.0"
```

Windows Registry change logs

```
#AO-WUA-Registry-Modified
Thu May 07 04:01:58 2015 WIN-2008-249.ersijiu.com 10.1.2.249 FortiSIEM-WUA-
Registry [monitorStatus]="Success" [regKeyPath]-
]="HKLM\\SOFTWARE\\Microsoft\\ExchangeServer\\v14\\ContentIndex\\CatalogHealth\\
{0d2a342a-0b15-4995-93db-d18c3df5860d}" [regValueName]="TimeStamp"
[regValueType]="1"
[osObjAction]="Modified" [oldRegValue]-
]="MgAwADEANQAtADAANQAtADAANwAgADAAMwA6ADQAOQA6ADQANwBaAAAA"
[newRegValue]="MgAwADEANQAtADAANQAtADAANwAgADAANAA6ADAAMQA6ADQAOABaAAAA"
#AO-WUA-Registry-Removed
Thu May 07 05:25:09 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-Registry [mon-
itorStatus]="Success"
[regKeyPath]="HKLM\\SOFTWARE\\RegisteredApplications" [regValueName]="Skype"
[regValueType]="1" [osObjAction]="Removed" [oldRegValue]-
="UwBPAEYAVABXAEEAUgBFAFwAQwBsAGkAZQBuAHQAcwBcAEkAbgB0AGUAcgBuAGUAdAAgAEMAYQBsAG-
wAXABTAGsAeQBwAGUAXABDAGEAcABhAGIAaQBsAGkAdABpAGUAcwBkAGgAZABoAGQAaABkAGgAZABoAGQ-
AAAA=" [newRegValue]=""
```

Windows WMI logs

```
#AO-WUA-WMI-Win32_Processor
Thu May 07 03:53:33 2015 WIN-2008-LAW-agent 10.1.2.242 FortiSIEM-WUA-WMI [mon-
itorStatus]="Success"  [__CLASS]="Win32_Processor"
[AddressWidth]="64" [Architecture]="9" [Availability]="3" [Caption]="Intel64 Fam-
ily 6 Model 26 Stepping 5" [ConfigManagerErrorCode]="" [Con-
figManagerUserConfig]="" [CpuStatus]="1" [CreationClassName]="Win32_Processor"
[CurrentClockSpeed]="2266" [CurrentVoltage]="33"
[DataWidth]="64" [Description]="Intel64 Family 6 Model 26 Stepping 5" [DeviceID]-
]="CPU0" [ErrorCleared]="" [ErrorDescription]=""
[ExtClock]="" [Family]="12" [InstallDate]="" [L2CacheSize]="0" [L2CacheSpeed]=""
[L3CacheSize]="0" [L3CacheSpeed]="0"
[LastErrorCode]="" [Level]="6" [LoadPercentage]="8" [Manufacturer]="GenuineIntel"
[MaxClockSpeed]="2266"
[Name]="Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz" [NumberOfCores]="1" [Num-
berOfLogicalProcessors]="1"
[OtherFamilyDescription]="" [PNPDeviceID]="" [PowerManagementCapabilities]=""
[PowerManagementSupported]="0"
[ProcessorId]="0FEBFBFF000106A5" [ProcessorType]="3" [Revision]="6661"
```

```
[Role]="CPU" [SocketDesignation]="CPU socket #0"
[Status]="OK" [StatusInfo]="3" [Stepping]="" [SystemCreationClassName]="Win32_Com-
puterSystem" [SystemName]="WIN-2008-LAW-AG"
UniqueId]="" [UpgradeMethod]="4" [Version]="" [VoltageCaps]="2"
```

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
- End point Security Software
- Mail Server
- Management Server/Appliance
- Remote Desktop
- 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
- 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	
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 **CMDB > Event Types**, search for "tomcat" in the **Device Type** and **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "tomcat" in the **Name** column to see the reports associated with this application or device.

Configuration

JMX

1. Add the necessary parameters to the Tomcat startup script.
   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" \
   ```
2. Edit the access authorization file `jmxremote.access.`

   ```
   monitorRole  readonly
   controlRole  readwrite
   ```
3. 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>
```

4. 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 'Discovering Infrastructure' and 'Setting Access Credentials for Device Discovery' under 'Chapter: Configuring FortiSIEM'.

Settings for Access Credentials

Settings for <device name><protocol name> Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Apache Tomcat application server over JMX, use these settings:

Setting	Value
Name	tomcat
Device Type	Apache Tomcat
Access Protocol	JMX
Pull Interval (minutes)	5
Port	9218
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]:[eventSever-
ity]=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,[webAp-
pName]=//localhost/host-manager,[servletName]=HTMLHostManager,[countAllocated]=0,
[totalRequests]=0,[reqErrors]=0,[loadTime]=0,[reqProcessTimeAvg]=0,[maxIn-
stances]=20,[servletState]=STARTED

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_SESSION]:[eventSever-
ity]=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,[expiredSes-
sion]=0,[rejectedSession]=0,[sessionLifetimeAvg]=0,[sessionLifetimePeak]=0,[ses-
sionProcessTimeMs]=0,[sessionCreateRate]=0,[sessionExpireRate]=0,
[webAppState]=STARTED,[processExpiresFrequency]=6,[maxSessionLimited]=-1,[maxIn-
activeInterval]=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-man-
ager,[dataSource]="jdbc/postgres1",[dbDriver]=org.postgresql.Driver,[act-
iveSessionsPeak]=20,[activeSessions]=0,[idleSessionsPeak]=10,[idleSessions]=0

<134>Jan 22 01:57:33 10.1.2.16 java: [PH_DEV_MON_TOMCAT_THREAD_POOL]:[eventSever-
ity]=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,[reqPro-
cessorName]="http-apr-18080",[recvBytes]=0,[sentBytes]=62748914,
[totalRequests]=4481,[reqProcessTimeAvg]=44107,[reqProcessTimeMax]=516,
[reqRate]=0,[reqErrors]=7
```

IBM WebSphere Configuration

- What is Discovered and Monitored
- 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

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
Syslog			Log analysis

Event Types

In **CMDB > Event Types**, search for "websphere" in the **Description** column 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.js
p,[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
```

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "websphere" in the **Name** column to see the reports associated with this device.

Configuration

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 need to 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	1. `${WebSphere_Home}/AppServer/runtimes/com.ibm.ws.admin.client.jar` 2. `${WebSphere_Home}/AppServer/plugins/com.ibm.ws.security.crypto.jar`
SSL files	1. `${WebSphere_Home}/AppServer/profiles/${Profile_Name}/etc/DummyClientKeyFile.jks` 2. `${WebSphere_Home}/AppServer/profiles/${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: 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*.

Settings for Access Credentials

Settings for IBM Websphere HTTPS Access Credentials When setting the **Access Method Definition** for letting FortiSIEM access your IBM Websphere device over HTTPS and SNMP, use these settings. When you are setting the **Device Credential Mapping Definition**, make sure to map both the HTTPS and SNMP credentials to the same IP address for your Websphere device. **HTTPS**

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

When setting the **Access Method Definition** for letting FortiSIEM access your IBM Websphere device over SNMP, use these settings. When you are setting 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

When setting the **Access Method Definition** for letting FortiSIEM access your IBM Websphere device over JMX, use these settings:

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 Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "asp.net" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "asp.net" in the **Name** column to see the reports associated with this application or device.

Configuration

WMI

Required WMI Class

For ASP.NET metrics, make sure that the WMI class `Win32_PerfFormattedData_ASPNET_ASPNET`is available on the ASP.NET server.

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 will need to use in setting 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
```

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**.

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,[aspReqDis-
connected]=0,[aspReqQueued]=0,[aspReqRejected]=0,[aspReqWaitTimeMs]=0
```

Oracle GlassFish Server Configuration

- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials
- Sample Event for Glassfish 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, Avg Request Processing time	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
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 **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	Performance Monitoring

Event Types

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, write: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "glassfish" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "glassfish" in the **Name** column 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 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*.

Settings for Access Credentials

Settings for Oracle GlassFish JMX Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Oracle GlassFish device over JMX, use these settings.

Setting	Value
Name	glassfish
Device Type	SUN Glassfish App Server
Access Protocol	JMX
Pull Interval (minutes)	5
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]:[eventSever-
ity]=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,[cach-
ingAllowed]=false,[linkingAllowed]=false,[crossContextAllowed]=true

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_CPU]:[eventSever-
ity]=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]:[eventSever-
ity]=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]:[eventSever-
ity]=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,[ses-
sionProcessTimeMs]=85,[sessionLifetimeAvg]=0,[sessionLifetimePeak]=0,[maxSes-
sionLimited]=-1,[maxInactiveInterval]=1800

<134>Jan 22 02:00:29 10.1.2.201 java: [PH_DEV_MON_GLASSFISH_SERVLET]:[eventSever-
ity]=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]:[eventSever-
ity]=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]:[eventSever-
ity]=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]:[eventSever-
ity]=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 Applic-
ation 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 Applic-
ation 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]:[eventSever-
ity]=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 Configuration

- What is Discovered and Monitored
- 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	Performance Monitoring

Protocol	Information discovered	Metrics collected	Used for
		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,	

Event Types

In **CMDB > Event Types**, search for "WebLogic in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "WebLogic" in the **Name** column 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 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*.

Settings for Access Credentials

Settings for Oracle WebLogic JMX Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Oracle WebLogic application server over JMX, use these settings.

- 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
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]:[eventSever-
ity]=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,[listenPortEn-
abled]=true,[sslListenPortEnabled]=true

<134>Jan 22 02:12:20 10.1.2.16 java: [PH_DEV_MON_WEBLOGIC_MEMORY]:[eventSever-
ity]=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]:[eventSever-
ity]=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,[webAp-
pName]=examplesServer_/console,[ser-
vletName]=/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]:[eventSever-
ity]=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]:[eventSever-
ity]=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]:[eventSever-
ity]=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,[ejbCom-
mitTransactions]=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]:[eventSever-
ity]=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,[webCon-
textRoot]=/jws_basic_simple,[activeSessions]=0,[activeSessionsPeak]=0,
[activeSessionTotal]=0,[numServlet]=4,[singleThreadedServletPool]=5
```

Redhat JBOSS Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "boss" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for jobs" in the **Name** column to see the reports associated with this application or device.

Configuration

JMX

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 need to 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 'Discovering Infrastructure' and 'Setting Access Credentials for Device Discovery' under 'Chapter: Configuring FortiSIEM'.

Settings for Access Credentials

Settings for Redhat JBOSS JMX Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your <device name> over <protocol>, use these settings:

Setting	Value
Name	jboss
Device Type	Redhat JBOSS App Server
Access Protocol	JMX
Pull Interval (minutes)	5
Port	8880

Setting	Value
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]:[eventSever-
ity]=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,[reqPro-
cessTimeAvg]=10472,[startTime]=1353919592,[cookiesAllowed]=true,[cach-
ingAllowed]=true,[linkingAllowed]=false,[crossContextAllowed]=true

<134>Feb 06 11:38:36 10.1.2.16 java: [PH_DEV_MON_JBOSS_SERVLET]:[eventSever-
ity]=PHL_INFO,[destIpAddr]=10.1.2.16,[hostIpAddr]=10.1.2.16,[hostName]=SH-WIN08R2-
JMX,[destDevPort]=1090,[appVersion]=6.1.0.Final "Neo",[webAp-
pName]=//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]:[eventSever-
ity]=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",[reqPro-
cessorName]=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]:[eventSever-
ity]=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 Configuration

FortiSIEM supports these authentication servers for discovery and monitoring.

- Cisco Access Control Server (ACS) Configuration
- Microsoft Internet Authentication Server (IAS) Configuration
- Juniper Networks Steel-Belted RADIUS Configuration
- Vasco DigiPass Configuration
- CyberArk Password Vault Configuration

Cisco Access Control Server (ACS)

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "cisco secure acs" in the **Device Type** and **Description** column 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 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 will need to use in setting 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

Report	CSV Attributes
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 • 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 syslogs 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 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.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Microsoft Internet Authentication Server (IAS) Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
WMI			
Syslog			

Event Types

In **CMDB > Event Types**, search for "microsoft isa" in the **Description** column 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

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 will need to use in setting 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 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.

Syslog

You need to 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 Manager to configure what information will be sent to FortiSIEM.

Juniper Networks Steel-Belted RADIUS 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 **CMDB > Event Types**, search for "Juniper Steel-Belted RADIUS" in the **Device Type** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Syslog

1. Login as administrator.
2. Install and configure Epilog application to convert log files written by Steelbelted RADIUS server into syslogs for sending to FortiSIEM:
    a. Download Epilog from Epilog download site 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 needs to 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.

Vasco DigiPass 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 **CMDB > Event Types**, search for "Vasco DigiPass" in the **Device Type** column 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

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

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 Loca-
tion: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:Ad-
ministration 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 Loca-
tion: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/}
```

CyberArk Password Vault Configuration

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 **CMDB > Event Types**, search for "CyberArk-Vault" in the **Device Type** column to see close to 400 event types associated with this device.

Rules

In **Analytics** > **Rules**, search for "CyberArk":

- 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 **Analytics** > **Reports**, search for "CyberArk":

- 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 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: Pro-
duct="Vault";Version="9.20.0000";MessageID="295";Message="Retrieve pass-
word";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
```

Database Server Configuration

FortiSIEM supports these database servers for discovery and monitoring.

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

IBM DB2 Server Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "db2" in the **Device Type** and **Description** column 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 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.

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

When setting the **Access Method Definition** for allowing FortiSIEM to access your <device name> over <protocol>, use these settings:

Setting	Value
Name	db2_linux
Device Type	IBM DB2
Access Protocol	JDBC
Used For	audit

Setting	Value
Pull Interval (minutes)	5
Port	50000
Database Name	
Audit Table	db2inst1.AUDIT
Checking Table	db2inst1.CHECKING
ObjMaint Table	db2inst1.OBJMAINT
SecMaint Table	db2inst1.SECMAINT
SysAdmin Table	db2inst1.SYSADMIN
Validate Table	db2inst1.VALIDATE
Context Table	db2inst1.CONTEXT
Execute Table	db2inst1.EXECUTE
User 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]:[eventSever-
ity]=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_Con-
nMgt_,[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,[dbEventCat-
egory]=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 Configuration

- Supported Versions
- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials
- Sample Events

Supported Versions

- SQL Server 2005
- SQL Server 2008
- SQL Server 2008 R2
- SQL Server 2012
- SQL Server 2014

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
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

Protocol	Information discovered	Metrics collected	Used for
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

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 and compliance

Event Types

In **CMDB > Event Types**, search for "sql server" in the **Device Name** and **Description** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for " sql server" in the **Name** column to see the rules associated with this application or device.

Reports

In **Analytics > Reports** , search for "sql server" in the **Name** column to see the reports associated with this application or device.

Configuration

SNMP

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

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 will need to use in setting 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**.

JDBC for Performance Monitoring

Creating an 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 to do so are not available on Linux. You have to create a separate user with read-only privileges.

Create a Read-Only User to Access System Tables

1. Log in to your SQL Server with an 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 and run these commands.
   Check to see if you get the same results with your read-only account as you do with your sa account.

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

3. The following additional configuration steps should be performed for the collection of Logon Failures.
   - For Server 2012 - https://technet.microsoft.com/en-us/library/ms175850(v=sql.110).aspx
   - For Server 2014 - https://technet.microsoft.com/sr-latn-rs/library/ms175850(v=sql.120)
   - For Server 2016 - https://msdn.microsoft.com/en-us/library/ms175850.aspx

JDBC for Database Audit Trail Collection

Creating a 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 to do so are not available on Linux. You have to create a separate user with read-only privileges.

Create a Read-Only User to Access System Tables

1. Log in to your SQL Server with an 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. Save the four SQL Server Scripts attached to this topic to **My Documents > SQL Server Management Studio > Projects** as four separate files.
3. Login to SQL Server Management Studio with an sa account.
4. Browse to and execute the **Database and Table Creation** script to create the database and tables.
5. Browse to and execute the **Logon Trigger Creation** script to create triggers.
   SQL Server introduced Logon Trigger in SQL Server 2005 SP2, so the database version must be greater than 2005 SP2 for logon trigger creation to succeed.
6. Browse to and execute the **DDL Server Level Trigger Creation** script to create database events.

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.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Settings for SQL Server JDBC Access Credentials for Performance Monitoring

When setting the **Access Method Definition** for allowing FortiSIEM to access your SQL Server over JDBC for performance monitoring, use these settings.

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**.

Setting	Value
Name	The name of the database instance you're creating the credential for
Device Type	Microsoft SQL Server
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

Settings for SQL Server JDBC Access Credentials for Database Audit Trail Collection

When setting the **Access Method Definition** for allowing FortiSIEM to access your SQL Server database instance over JDBC for database audit trail collection, use these settings.

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**.

Setting	Value
Name	The name of the database instance you're creating the credential for

Setting	Value
Device Type	Microsoft SQL Server
Access Protocol	JDBC
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

Creating a Database Truncate Script

Since audit 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 ?';
```

7. Click **OK**.
8. 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**.

Sample Events

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,[dbLo-
gFileUsedKB]=26326,[dbLogGrowthCount]=4,[dbLogShrinkCount]=0,[dbLo-
gFlushPerSec]=1.69,[dbTransPerSec]=4.44,
[dbDeadLocksPerSec]=0,[dbLogCacheHitRatio]=60.01,[dbUserConn]=16,[dbTar-
getServerMemoryKB]=1543232,[dbTotalServerMemoryKB]=1464760,[dbPageSplit-
sPerSec]=0.45,
[dbPageWritesPerSec]=0.01,[dbLatchWaitsPerSec]=0.77,[dbPageReadsPerSec]=0.01,
[dbFullScansPerSec]=1.83,[dbBufferCacheHitRatio]=100,[dbCount]=8,[dbUserCount]=25,
[dbLoggedinUserCount]=2,[dbPagesInBufferPool]=116850,[dbPagesFreeInBuffer-
Pool]=2336,[dbAverageWaitTimeMs]=239376,
[appVersion]=Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64),[server-
Name]=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,[dbLo-
gShrinkCount]=0,[dbTransPerSec]=0.96,[dbLogFlushPerSec]=0.01,[dbLo-
gCacheHitRatio]=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,[dbS-
ize]= 3.0,[dbowner]= sa,[dbId]= 2,[dbcreated]= 1321545600,
[dbstatus]= Status=ONLINE; Updateability=READ_WRITE; UserAccess=MULTI_USER; Recov-
ery=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),[server-
Name]= 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, [srcAp-
p]=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.MSrep-
lication_options(optname);, [schemaName]=dbo, [objType]=INDEX, [destName]=WIN-
S2EDLFIUPQK, [destPort]=1433
```

Microsoft SQL Server Scripts

SQL Server Trigger Creation Script (PH_LogonEventsTrigger.sql)

This script is to create a server level trigger called `PH_LoginEvents`. It will record all logon events when a user establishes a session to the database server. The trigger locates at the **database server > Server Objects > Triggers**.

```
CREATE TRIGGER PH_LoginEvents
ON ALL SERVER WITH EXECUTE AS self
FOR LOGON
AS
BEGIN
DECLARE @event XML
SET @event = EVENTDATA()
INSERT INTO PH_Events.dbo.LogonEvents (EventTime,EventType,SPID,Server-
Name,LoginName,LoginType,SID,HostName,IsPooled,AppName,XMLEvent)
VALUES(CAST(CAST(@event.query('/EVENT_INSTANCE/PostTime/text()') AS VARCHAR(64))
AS DATETIME),
       CAST(@event.query('/EVENT_INSTANCE/EventType/text()') AS VARCHAR(128)),
       CAST(@event.query('/EVENT_INSTANCE/SPID/text()') AS VARCHAR(128)),
       CAST(@event.query('/EVENT_INSTANCE/ServerName/text()') AS VARCHAR(128)),
       CAST(@event.query('/EVENT_INSTANCE/LoginName/text()') AS VARCHAR(128)),
       CAST(@event.query('/EVENT_INSTANCE/LoginType/text()') AS VARCHAR(128)),
       CAST(@event.query('/EVENT_INSTANCE/SID/text()') AS VARCHAR(128)),
       CAST(@event.query('/EVENT_INSTANCE/ClientHost/text()') AS VARCHAR(128)),
       CAST(@event.query('/EVENT_INSTANCE/IsPooled/text()') AS VARCHAR(128)),
       APP_NAME(),
       @event)
END;
```

SQL Server Table Creation Script (PH_EventDB_Tables_Create.sql)

```
CREATE DATABASE PH_Events

GO
CREATE TABLE PH_Events.dbo.DDLEvents
(
    XMLEvent XML,
    DatabaseName VARCHAR(64),
    EventTime DATETIME DEFAULT (GETDATE()),
    EventType VARCHAR(128),
    SPID VARCHAR(128),
    ServerName VARCHAR(128),
    LoginName VARCHAR(128),
    ObjectName VARCHAR(128),
    ObjectType VARCHAR(128),
    SchemaName VARCHAR(128),
    CommandText VARCHAR(128)
)

GO
CREATE TABLE PH_Events.dbo.LogonEvents
(
    XMLEvent XML,
    EventTime DATETIME,
    EventType VARCHAR(128),
    SPID VARCHAR(128),
    ServerName VARCHAR(128),
    LoginName VARCHAR(128),
    LoginType VARCHAR(128),
    SID VARCHAR(128),
    HostName VARCHAR(128),
    IsPooled VARCHAR(128),
    AppName VARCHAR(255)
)
```

SQL Server DDL Event Creation Script (PH_DDL_Server_Level_Events.sql)

```
CREATE TRIGGER PH_DDL_Server_Level_Events
ON ALL SERVER

FOR DDL_ENDPOINT_EVENTS, DDL_LOGIN_EVENTS, DDL_GDR_SERVER_EVENTS, DDL_
AUTHORIZATION_SERVER_EVENTS,
CREATE_DATABASE, ALTER_DATABASE, DROP_DATABASE
/**FOR DDL_SERVER_LEVEL_EVENTS**/
AS
DECLARE @eventData AS XML;
SET @eventData = EVENTDATA();
/**declare @eventData as XML;
set @eventData = EVENTDATA();**/
insert into PH_Events.dbo.DDLEvents(EventTime, EventType, SPID, ServerName,
LoginName, ObjectName, ObjectType, SchemaName, DatabaseName, CommandText,
XMLEvent)
values(cast(@eventData.query('data(//PostTime)') as varchar(64)),
       cast(@eventData.query('data(//EventType)') as varchar(128)),
       cast(@eventData.query('data(//SPID)') as varchar(128)),
       cast(@eventData.query('data(//ServerName)') as varchar(128)),
       cast(@eventData.query('data(//LoginName)') as varchar(128)),
       cast(@eventData.query('data(//ObjectName)') as varchar(128)),
       cast(@eventData.query('data(//ObjectType)') as varchar(128)),
       cast(@eventData.query('data(//SchemaName)') as varchar(128)),
       cast(@eventData.query('data(//DatabaseName)') as varchar(64)),
       cast(@eventData.query('data(//TSQLCommand/CommandText)') as varchar(128)),
     /**  DB_NAME(),**/
       @eventData);
```

SQL Server Database Level Event Creation Script (PH_Database_Level_Events.sql)

```
USE master;
GO
CREATE TRIGGER PH_Database_Level_Events
on DATABASE
FOR DDL_DATABASE_LEVEL_EVENTS
AS
DECLARE @eventData AS XML;
SET @eventData = EVENTDATA();
INSERT INTO PH_Events.dbo.DDLEvents(EventTime, EventType, SPID, ServerName,
LoginName, ObjectName, ObjectType, SchemaName, DatabaseName, CommandText,
XMLEvent)
VALUES(cast(@eventData.query('data(//PostTime)') as varchar(64)),
       cast(@eventData.query('data(//EventType)') as varchar(128)),
           cast(@eventData.query('data(//SPID)') as varchar(128)),
           cast(@eventData.query('data(//ServerName)') as varchar(128)),
       cast(@eventData.query('data(//LoginName)') as varchar(128)),
       cast(@eventData.query('data(//ObjectName)') as varchar(128)),
           cast(@eventData.query('data(//ObjectType)') as varchar(128)),
           cast(@eventData.query('data(//SchemaName)') as varchar(128)),
           cast(@eventData.query('data(//DatabaseName)') as varchar(64)),
           cast(@eventData.query('data(//TSQLCommand/CommandText)') as varchar
(128)),
       @eventData
);
```

MySQL Server

- What is Discovered and Monitored
- 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
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

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "mysql" in the **Device Type** and **Description** columns to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "mysql" in the **Name** column to see the rules associated with this application or device.

Reports

In **Analytics > Reports** , search for ""mysql" in the **Name** and **Description** columns 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

JDBC for Database Auditing - MySQL Server

You need to 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.

1. Start MySQL server with TABLE output enabled.

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

2. Login to mysql, 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 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.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>

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

Settings for MySQL Server JBDC Access Credentials for Performance Monitoring

When setting the **Access Method Definition** for allowing FortiSIEM to access your MySQL Server over JDBC for performance monitoring, use these settings.

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

When setting the **Access Method Definition** for allowing FortiSIEM to access your MySQL Server over JDBC for database auditing, use these settings.

Setting	Value
Name	MySQL-Audit
Device Type	Oracle MySQL
Access Protocol	JBDC
Used For	Audit

Setting	Value
Pull Interval (minutes)	5
Port	3306
Database Name	mysql
Audit Table	general_log
User Name	The administrative user for the database server
Password	The password associated with the administrative user

Sample events

System Level Performance Metrics

```
<134>Apr 21 19:06:07 10.1.2.8 java: [PH_DEV_MON_PERF_MYSQLDB]: [eventSever-
ity]=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
```

System Level Performance Metrics

```
<134>Apr 21 19:06:07 10.1.2.8 java: [PH_DEV_MON_PERF_MYSQLDB]: [eventSever-
ity]=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
```

Logon/Logoff Events

```
<134>Apr 29 15:14:54 abc-desktop java: [MYSQL_ Logon_Success]: [eventSever-
ity]=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]: [eventSever-
ity]=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 sli-
utest

<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 sli-
utest
```

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 tutori-
als_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 tutori-
als_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 tutori-
als_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 sli-
utable
```

Oracle Database Server Configuration

- Supported Versions
- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials
- Sample Events

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,	

Protocol	Information discovered	Metrics collected	Used for
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**	
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 **CMDB > Event Types**, search for "oracle database" in the **Description** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "oracle database" in the **Description** column to see the rules associated with this application or device.

Reports

In **Analytics > Reports** , search for "oracle database" in the **Name** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

JDBC for Database Performance Monitoring - Oracle Database Server

To configure your Oracle Database Server for performance monitoring by FortiSIEM, you need to 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.

```
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;
```

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
    1. Download Epilog from Epilog download site and install it on your Windows Server.
    2. Launch Epilog from Start→All Programs→InterSect Alliance→Epilog for windows
    3. Configure Epilog application as follows
        a. 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**.
        b. Click Add button to add Oracle Alert log file to be sent to FortiSIEM. **Also make sure the Log Type is OracleAlertLog**.
        c. After adding both the files, SNARE Log Configuration will show both the files included as follows
        d. 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.
        e. 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 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.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>

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

Settings for Oracle Database Server JDBC Access Credentials for Performance Monitoring

When setting the **Access Method Definition** for allowing FortiSIEM to access your Oracle database server over JDBC, use these settings.

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

```
[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 - Pro-
duction, [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,[dbSharedPoolFreeRa-
tio]=18.55,[dbSessionCount]=40,[dbIOKBytesPerSec]=33.26,[dbRequestsPerSec]=3.24,
```

```
[dbSystemTablespaceUsage]= 2.88,[dbTempTablespaceUsage]= 0,[dbUser-
sTablespaceUsage]= 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] 'ter-
minal' 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$TEXT:
[99] Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST-
T=10.90.217.247)(PORT=4566)) PRIV$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-
D=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 Configuration

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

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

Infoblox DNS/DHCP Configuration

- 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, 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	

Protocol	Information discovered	Metrics collected	Used for
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 **CMDB > Event Types**, search for "infoblox" in the **Device Type** and **Description** columns to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "infoblox" in the **Name** and **Description** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

ISC BIND DNS Configuration

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

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "isc bind" in the **Device Type** and **Description** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Syslog

Configure the ISC BIND DNS Server to Send Syslogs

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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "linux dhcp" in the **Device Type** column 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. 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:
    1. Define the community string for FortiSIEM usage and permit snmp access from FortiSIEM IP.
    2. Allow FortiSIEM to (read-only) view the mib-2 tree.
    3. 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 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*.

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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Microsoft DHCP (2003, 2008) Configuration

- What is Discovered and Monitored
- Configuration
- Settings for Access Controls

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
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 **CMDB > Event Types**, search for "microsoft dhcp" in the **Description** column 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

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

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 will need to use in setting 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 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*.

Syslog

1. Log into your Microsoft DHCP server as an administrator.
2. Go to **Start > Administrative Tools > DHCP**.
3. Select the DHCP server you want to monitor, then right-click and select **Properties**.
4. Click the **General** tab, and then select **Enable DHCP audit logging**.
5. Click the **DNS** tab, and then select **Dynamically update DNS A and PTR records only if requested by the DHCP clients** and **Discard A and PTR records when lease is deleted**.
6. Click the **Advanced** tab.
7. Set **Audit log file path** to `C:\WINDOWS\system32\dhcp.`
8. Set **Database path** to `C:\\WINDOWS\system32\dhcp.`
9. Set **Backup path** to `C:\\WINDOWS\System32\dhcp\backup.`
10. Clock **OK** to complete configuration.

Use the Windows Agent Manager to further configure sending syslogs from your device to FortiSIEM.

Sample Microsoft DHCP Syslog

```
 <15>May 27 17:22:43 ADS-Pri.ACME.net WinDHCPLog        0

11,05/27/08,17:22:43,Renew,192.168.20.46,Lucy-XPS.ACME.net,009096F27636,
 <15>Jun 20 12:20:58 ADS-Pri.ACME.net WinDHCPLog       0
10,06/20/08,12:20:58,Assign,192.168.20.35,mission.,000D5639076C,
 <13>Mar 29 10:25:28 192.168.0.10 WinDHCPLog 0

30,03/29/10,10:25:27,DNS Update Request,40.20.168.192,John-lap.ACME.net,,
 <13>Mar 29 10:25:05 192.168.0.10 WinDHCPLog 0

32,03/29/10,10:25:01,DNS Update Successful,192.168.20.32,Mary-laptop.ACME.net,,
 <13>Jun  1 14:24:08 192.168.0.10 WinDHCPLog   0

31,06/01/10,14:24:08,DNS Update Failed,192.168.26.31,Joe-LAPTOP.ACME.net,-1,
 <13>Jun  1 14:24:08 192.168.0.10 WinDHCPLog   0

25,06/01/10,14:24:07,0 leases expired and 1 leases deleted,,,,
```

Settings for Access Controls

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>

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

Microsoft DNS (2003, 2008) Configuration

- What is Discovered and Monitored
- 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 (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

Protocol	Information discovered	Metrics collected	Used for
Syslog	Application type	**DNS name resolution activity**: DNS Query Success and Failure by type	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "microsoft dans" in the **Description** column 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

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

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 will need to use in setting 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 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*.

Syslog

Use the Windows Agent Manager to configure sending syslogs from your device to FortiSIEM.

Sample Windows DNS Syslog

```
<13>Aug 10 19:14:36 192.168.20.99 MSDNSLog 0 20090810 19:13:43 15EC PACKET
025AED90 UDP Rcv 192.168.20.35 b66e Q [0001 D NOERROR] A (12)autodiscover(8)ac-
celops(3)net(0)
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Directory Server Configuration

FortiSIEM supports these directory servers for discovery and monitoring.

- Microsoft Active Directory Configuration

Microsoft Active Directory Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics collected	Used for
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	
WMI		"repadmin /replsummary" command output - detect replication statistics	

Event Types

- 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

Required WMI Class

For Active Directory metrics, make sure that this WMI class is available on the Active Directory server.

`Win32_PerfRawData_NTDS_NTDS`

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 will need to use in setting 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 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.

Document Management Server Configuration

FortiSIEM supports these document management servers for discovery and monitoring.

- Microsoft SharePoint Configuration

Microsoft SharePoint Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
WMI		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 **CMDB > Event Types**, search for "sharepoint" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "sharepoint" in the **Name** column 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 needs to 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

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 will need to use in setting 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**.

Mail Server Configuration

FortiSIEM supports these mail servers for discovery and monitoring.

- Microsoft Exchange Configuration

Microsoft Exchange Configuration

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

What is Discovered and Monitored

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

Protocol	Information discovered	Metrics collected	Used for
WMI		**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	Performance Monitoring

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):	
WMI		Application Logs	Security Monitoring and Compliance

Event Types

In **CMDB > Event Types**, search for "microsoft exchange" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "microsoft exchange" in the **Name** column to see the reports associated with this application or device.

Configuration

SNMP

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

Required WMI Classes

For Exchange metrics, make sure that these WMI classes are available on the Exchange server.

- `Win32_PerfRawData_MSExchangeIS_MSExchangeIS`
- `Win32_PerfRawData_MSExchangeIS_MSExchangeISMailbox`
- `Win32_PerfRawData_MSExchangeIS_MSExchangeISPublic`
- `Win32_PerfRawData_SMTPSVC_SMTPServer`
- `Win32_PerfFormattedData_ESE_MSExchangeDatabase`
- `Win32_PerfFormattedData_ESE_MSExchangeDatabaseInstances`
- `Win32_PerfFormattedData_MSExchangeMailSubmission_MSExchangeMailSubmission`
- `Win32_PerfFormattedData_MSExchangeStoreInterface_MSExchangeStoreInterface`
- `Win32_PerfFormattedData_MSExchangeReplication_MSExchangeReplication`
- `Win32_PerfFormattedData_MSExchangeTransportQueues_MSExchangeTransportQueues`

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 will need to use in setting 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 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.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Management Server/Appliance Configuration

FortiSIEM supports these web servers for discovery and monitoring.

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

Cisco Application Centric Infrastructure (ACI) Configuration

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 **CMDB > Event Types** and search for "Cisco_ACI".

Rules

Go to **CMDB > Rules** and search for "Cisco ACI".

Reports

Go to **CMDB > Reports** and search for "Cisco ACI".

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. Click **New** and create a credential as follows
    a. **Name** - enter a name
    b. **Device Type** - set to Cisco Cisco ACI
    c. **Access Protocol** - set to Cisco APIC API
    d. **Password Configuration** - set to Manual
    e. Set **User Name** and **Password** for the various REST API
    f. Click **Save**
3. Create an **IP to Credential Mapping**
    1. IP - specify the IP address of the ACI Controller
    2. **Credential** - specify the Name as in 2a
4. **Test Connectivity** - Run Test Connectivity with or without ping and make sure the test succeeds
5. Check **Pull Events** tab to make sure that a event pulling entry is created

Sample Events

Overall Health Event


```
[Cisco_ACI_Overall_Health]: {"attributes":{"childAc-
tion":"","cnt":"29","d-
n":"topology/HDfabricOverallHealth5min0","healthAvg":"82","healthMax":"89",

"healthMin":"0","healthSpct":"0","healthThr":"","healthTr":"1","in-
dex":"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":{"childAc-
tion":"","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":
{"childAc-
tion":"","chng":"0","-
cur":"100","maxSev":"cleared","prev":"100","rn":"health","status":"",

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


Nodes Health Event


```
[Cisco_ACI_Node_Health]: {"attributes":{"address":"10.0.208.95","childAc-
tion":"","configIssues":"","currentTime":"2016-09-05T08:15:51.794+00:00","d-
n":"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-ser-
vice","status":"","systemUpTime":"00:00:27:05.000"},"children":[{"healthInst":
{"attributes":{"childAction":"","chng":"-10","-
cur":"90","maxSev":"cleared","-
prev":"100","rn":"health","status":"","twScore":"90","updTs":"2016-09-
05T07:50:08.415+00:00"}}}]
```


Cluster Health Event


```
[Cisco_ACI_Cluster_Health]: {"attributes":{"addr":"10.0.0.1","adminSt":"in-ser-
vice","chassis":"10220833-ea00-3bb3-93b2-ef1e7e645889","childAc-
tion":"","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":{"childAc-
tion":"","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":"ac-
cess","ownerKey":"","ownerTag":"","prio":"unspecified","status":"","uid":"0"},

"children":[{"healthInst":{"attributes":{"childAc-
tion":"","chng":"0","-
cur":"100","maxSev":"cleared","prev":"100","rn":"health","status":"","twScore":

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


EPG Health Event


```
[Cisco_ACI_EPG_Health]: {"attributes":{"childAc-
tion":"","configIssues":"","configSt":"applied","descr":"","dn":"uni/tn-infra/ap-
access/epg-default","isAt-
trBasedEPg":"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":"","trig-
gerSt":"triggerable","txId":"5764607523034234882","uid":"0"},"children":
[{"healthInst":{"attributes":
{"childAc-
tion":"","chng":"0","-
cur":"100","maxSev":"cleared","prev":"100","rn":"health","status":"",

"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","deleg-
ated":"no","delegatedFrom":"","descr":

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

"lc":"soak-
ing","-
modTs":"never","occur":"1","origSeverity":"critical","prevSeverity":"critical",

"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_dhcp-
d,leCnnct:undefined,leNonOptCnt:undefined,leNotCnnct:undefined,name:ifc_dhcp-
d","childAction":"","code":"E4204979","created":"2016-09-
```

05T07:57:37.024+00:00","descr":"Allshardsofserviceifc_dhcp-dhaveconnectivitytotheleaderreplicaintheCluster.","dn":"subj-[topology/pod-1/node-2/lon/svc-ifc_dhcpd]/rec-8589934722","id":"8589934722","ind":"state-trans-ition","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":"un-known","changeSet":"","childAction":"","clientTag":"","code":"generic","created"

:"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":"spe-cial","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":"trans-ition","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":"cre-ation","modTs":"never","severity":"info","status":"","trig":"config","txId":

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

Fortinet FortiManager Configuration

- What is Discovered and Monitored
- 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

Please configure the device so that FortiSIEM can access it via SNMP.

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.

Remote Desktop Configuration

FortiSIEM supports these remote desktop applications for discovery and monitoring.

- Citrix Receiver (ICA) Configuration

Citrix Receiver (ICA) Configuration

- What is Discovered and Monitored
- Event Types
- Rules
- 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 **CMDB > Event Types**, search for "citrix ICA" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "citrix ICA" in the **Name** column to see the reports associated with this application or device.

Configuration

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 will need to use in setting 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 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.

Unified Communication Server Configuration

FortiSIEM supports these VoIP servers for discovery and monitoring.

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

Avaya Call Manager Configuration

- What is Discovered and Monitored
- Configuration
- 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

Rules

None

Reports

None.

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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

SFTP

SFTP is used to send Call Description Records (CDRs) 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. 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, they only have 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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cisco Contact Center Configuration

- What is Discovered and Monitored
- 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 **Analytics > Rules**, search for "cisco contact center" in the **Name** column to see the rules associated with 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM >

Discovering Infrastructure > Setting Access Credentials for Device Discovery 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Presence Server Configuration

- What is Discovered and Monitored
- 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

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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Tandeberg Telepresence Video Communication Server (VCS) Configuration

- What is Discovered and Monitored
- 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.

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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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) Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "cisco telepresence" in the **Description** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cisco Telepresence Video Communication Server Configuration

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 **CMDB > Event Types**, search for "Cisco-TVCS" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined reports for this device.

Reports

There are no predefined reports for this device.

Cisco Unity Connection Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "cisco unity" in the **Description** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "cisco unity" in the **Name** column to see the rules associated with 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Web Server Configuration

FortiSIEM supports these web servers for discovery and monitoring.

- Apache Web Server Configuration
- Microsoft IIS for Windows 2000 and 2003 Configuration
- Microsoft IIS for Windows 2008 Configuration
- Nginx Web Server Configuration

Apache Web Server Configuration

- What is Discovered and Monitored
- 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
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 **CMDB > Event Types**, search for "apache" in the **Device Type** and **Description** column to see the event types associated with this device.

Rules

here are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "apache" in the **Name** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

HTTPS

To communicate with FortiSIEM over HTTPS, you need to 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`.

   Modify the file as shown in these code blocks, depending on whether you are connecting over HTTP without authentication, or over HTTPS with authentication.
3. **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.
   1. Go to `/etc/httpd`, and if necessary, create an `account` directory.
   2. In the `account` directory, create two files, `users` and `groups`.

3. In the `groups` file, enter `admin:admin`.
4. 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 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.

Syslog

Install and configure Epilog application to send syslog to FortiSIEM

1. Download Epilog from Epilog download site and install it on your Windows Server.
2. For Windows, launch Epilog from Start→All Programs→InterSect Alliance→Epilog for windows
3. For Linux, type http://<yourApacheServerIp>:6162
4. Configure Epilog application as follows
   a. Go to Log Configuration. Click 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 need to 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; Win-
dows 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

When setting the **Access Method Definition** for allowing FortiSIEM to access your Apache web server over https, use these settings.

Setting	Value
Name	Apache-https
Device Type	generic
Access Protocol	HTTP or HTTPS
Port	80 (HTTP) or 443 (HTTPS)
URL	server-status?auto

Setting	Value
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 Configuration

- What is Discovered and Monitored
- 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
Syslog	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 **CMDB > Event Types**, search for "microsoft is" in the **Description** column 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

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

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 will need to use in setting 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 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'.

Syslog

Use Windows Agent Manager to configure the sending of syslogs from this device.

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;+r-
v: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 - - - -
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Microsoft IIS for Windows 2008 Configuration

- What is Discovered and Monitored
- Configuration
- Setting 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
Syslog	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 **CMDB > Event Types**, search for "microsoft is" in the **Description** column 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

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

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 will need to use in setting 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 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.

Syslog

Use the Windows Agent Manager to configure sending syslogs from your device to FortiSIEM.

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;+r-
v: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 - - - -
```

Setting Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Nginx Web Server Configuration

- What is discovered and monitored
- Configuration

The following protocols are used to discover and monitor various aspects of 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 **CMDB > Event Types**, search for "nginx" in the **Device Type** and **Description** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Syslog

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

- For **Syslog Server,** or the server where the syslogs 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.jp-g","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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Configuration
- HP BladeSystem Configuration

Cisco UCS Server Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "cisco us" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "cisco us" in the **Name** column 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 'Discovering Infrastructure' and 'Setting Access Credentials for Device Discovery' under 'Chapter: Configuring FortiSIEM'.

Settings for Access Credentials

Settings for Cisco UCS Server API Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Cisco UCS Server over the API, use these settings:

Setting	Value
Name	ucs
Device Type	Cisco UCS
Access Protocol	UCS API
Pull Interval (minutes)	5
Port	8880
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

```
[PH_DEV_MON_UCS_HW_PSU_STAT]:[eventSeverity]=PHL_INFO,[hostName]=machine,[hostIpAd-
dr]=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,[out-
putCurrentAvgAmp]=20.261436,[outputCurrentMaxAmp]=24.509804,
[outputCurrentMinAmp]=15.686275,[outputPowerWatt]=191.188004,[out-
putPowerAvgWatt]=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, [inputCur-
rentMaxAmp]=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,[inputPower-
MaxWatt]=7.843137,[inputPowerMinWatt]=7.843137,
outputPowerWatt]=0.000000,[outputPowerAvgWatt]=0.000000,[out-
putPowerMaxWatt]=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,[envTem-
pdDegC]=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,[hostIpAd-
dr]=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 Configuration

- What is Discovered and Monitored
- Configuration

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

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 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 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.

Cloud Applications

FortiSIEM supports these cloud applications for monitoring.

- AWS Access Key IAM Permissions and IAM Policies
- AWS CloudTrail API Configuration
- AWS EC2 CloudWatch API Configuration
- AWS RDS Configuration
- Box.com Configuration
- Cisco FireAMP Cloud Configuration
- Microsoft Azure AuditTrail Configuration
- Okta Configuration
- Salesforce CRM Audit Configuration

AWS Access Key IAM Permissions and IAM Policies

In order 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

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 will need to add permissions before you can actually add them in FortiSIEM.

Change permissions for IAM user

1. Select the user aomonitoring
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 specificy a more restricted policy as described in the next step.
6. Now, 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 API Configuration

- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials
- Sample Events for AWS CloudTrail

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
CloudTrail API	None	None	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "Cloudtrail" in the **Device Type** column 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.

Rules

There are no predefined rules for this device. However,

Reports

In **Analytics > Reports**, search for "cloudtrail" in the **Name** column 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.

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 **No** for **Apply Trail to all regions**

   You will need to create a cloudtrail for each region by following all the steps mentioned here for cloudtrail, SQS, and SNS. You cannot use 'Apply Trail to all regions' to collect trails for all regions in one

S3 bucket and have FortiSIEM pull these logs. In the future, FortiSIEM will be enhanced to support this capability

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	256KB
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. Select **Topics**
3. Select the SNS topic `snsaocloudtrail` that you specified when creating a cloudtrail
4. Click **Actions > Subscribe to topic** from the menu to launch the popup **Create Subscription**.
5. For **Protocol**, select **Amazon SQS**.
6. For **Endpoint**, enter the **ARN** of the queue that you created when setting up SQS.
7. 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**.

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.

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 Wizard > Event Pulling**.

Settings for Access Credentials

Settings for AWS CloudTrail API Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access the CloudTrail API, use these settings.

Setting	Value
Name	`aocloudtrail`
Device Type	Amazon AWS CloudTrail
Access Protocol	Amazon AWS CloudTrail
Region	Region where your AWS instance is located
Bucket	The name of the S3 bucket you created (`s3aocloudtrail`)
SQS Queue URL	Enter the ARN of your queue without the `http://` prefix
Access Key ID	The access key for your AWS instance
Secret Key	The secret key for your AWS instance

Setting	Value
Name	`aocloudtrail`
Device Type	Amazon AWS CloudTrail

Setting	Value
Access Protocol	Amazon AWS CloudTrail
Region	Region where your AWS instance is located
Bucket	The name of the S3 bucket you created (`s3aocloudtrail`)
SQS Queue URL	Enter the ARN of your queue without the `http://` prefix
Access Key ID	The access key for your AWS instance
Secret Key	The secret key for your AWS instance

Sample Events for AWS CloudTrail

```
Fri Oct 10 14:44:23 2014 FortiSIEM-CloudTrail
    [additionalEventData/LoginTo]=https://console.aws.amazon.com/console/home?state=hashAr
    gs%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
```

AWS EC2 CloudWatch API Configuration

- What is Discovered and Monitored
- Configuration
- Settings for Access Credentials
- Sample events

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	• 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)	Performance Monitoring

Event Types

- PH_DEV_MON_EBS_METRIC captures EBS metrics

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for 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.

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'. You should also be sure to read the topic Discovering Amazon Web Services (AWS) Infrastructure.

Settings for Access Credentials

Settings for AWS CloudWatch Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access AWS CloudWatch, use these settings.

Setting	Value
Name	ec2
Device Type	Amazon AWS EC2
Access Protocol	AWS SDK
Region	The region in which your AWS instance is located
Access Key ID	The access key for your EC2 instance
Secret Key	The secret key for your EC2 instance

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,[hostIpAd-
dr]=10.144.18.131,[cpuUtil]=0.334000,[diskReadKBytesPerSec]=0.000000,
[diskWriteKBytesPerSec]=0.000000,[diskReadReqPerSec]=0.000000,[diskWriteReqPer-
Sec]=0.000000,[sentBytes]=131,[recvBytes]=165,[sentBitsPerSec]=17.493333,[recvBit-
sPerSec]=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.com-
pute.amazonaws.com,[hostIpAddr]=172.30.0.50,[diskName]=/dev/sda1,[volumeId]=vol-
63287d9f,[diskReadKBytesPerSec]=7.395556,[diskWriteKBytesPerSec]=7.395556,[ioRead-
sPerSec]=0.000000,[ioWritesPerSec]=0.010000,[diskQLen]=0,[phLogDetail]=
```

AWS RDS Configuration

- What is Discovered and Monitored
- Configuration

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

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for 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.

Discovering AWS RDS

1. Create a AWS credential
   a. Go to Admin > Credentials > Step 1: Enter Credentials.
   b. Click **Add**.
      i. Set **Device Type** to Amazon AWS RDS.
      ii. Set **Access Protocol** as AWS SDK.
      iii. Set **Region** as the region in which your AWS instance is located.
      iv. Set **Access Key ID** as the access key for your EC2 instance.
      v. Set **Secret Key** as the secret key for your EC2 instance.

c. Click **Save**.

2. Create a IP to credential mapping
    1. Set **IP/IP Range** to amazon.com
    2. Choose **Credentials** to the one created in Step 1b.
3. Click test Connectivity to make sure the credential is working correctly.
4. Go to Admin > Discovery:
    1. Set **Discovery Type** as AWS Scan.
    2. Click OK to Save.
    3. Select the entry and Click **Discover**.
5. After Discovery finishes, check CMDB > 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,[dbEn-
queueDeadlocksPerSec]=0.000587,[freeMemKB]=489,[freeDiskMB]=4555,[swapMemUtil]-
]=0.000000,[ioReadsPerSec]=0.219985,[ioWritesPerSec]=0.213329,
[devDiskRdLatency]=0.08,[devDiskWrLatency]=0.4029,[phLogDetail]=
```

Box.com Configuration

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

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Box.com API	• Ccreation, deletion, and modification activity for specific files or folders • File-sharing properties, including whether the file is shared, password protected, or preview/download enabled, and how many times the file was downloaded or viewed		

Event Types

In **CMDB > Event Types**, search for "box.com" and look for **BOX** events in the **Name** column 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 can monitor a directory or subdirectory, for example `/All Files` or `/All Files/my files`, or a single file , for example `/All Files/my files/user guide.pdf`. When you set up the access credentials for FortiSIEM to communicate with Box.com, you provide the path to the folder or files you want to monitor, so you should have your Box.com storage set up before you set up your access credentials. You also won't need to initiate discovery of Box.com as you would with other devices, but should go to to **Admin > Setup wizard > Event Pulling** and make sure that a Box.com event pulling job is created after you have successfully set up access credentials.

Settings for Access Credentials

Settings for Box.com API Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access the Box.com API, use these settings.

Reauthorizing Access to Box.com

If FortiSIEM loses connectivity to Box.com, for example if an access token expires, you can edit the original credential and click **Re-authorize on Box.com**. This button is available only after you have created and saved a Box.com access credential for the first time.

Setting	Value
Name	BOX
Device Type	Box.com Box
Access Protocol	Box API
File Type	Select Folder or File
File/Directory Path	The path to the file or directory you want to monitor
Box.com Account	The email address for your Box.com account
Password	The password associated with the administrative user

When you click **Save**, you will be redirected to the Box.com website.

1. Enter your login credentials for Box.com.
2. Click **Authorize**.
3. Click **Grant access to Box**.
   You should see a message that the authorization for FortiSIEM to access your Box.com account was successful.
4. Follow the rest of the instructions in Setting Access Credentials for Device Discovery for associating the IP address of your Box.com account with the access credentials you created.

Sample Box.com Events

```
//the following event is generated when a folder called share was created using
the box.usage@gmail.com account
[PH_DEV_MON_BOX_FILE_CREATE]:[eventSeverity]=PHL_INFO,[fileName]=phBoxAgent.cpp,
[lineNumber]=625,[fileType]=folder,
[targetName]=share,[fileSize64]=0,[filePath]=/All Files,[fileOwner]=box usage,
[fileDesc]=,[user]=box usage,
[userId]=225282673,[accessTime]=1412700374,[accountName]=box.usage@gmail.com,
[fileId]=2541809279,[fileVersion]=1,
[targetHashCode]=,[phLogDetail]=

//the following event is generated when a file called  All Files/share/b.txt was
created using the box.usage@gmail.com account
[PH_DEV_MON_BOX_FILE_CREATE]:[eventSeverity]=PHL_INFO,[fileName]=phBoxAgent.cpp,
[lineNumber]=625,[fileType]=file,
[targetName]=b.txt,[fileSize64]=0,[filePath]=/All Files/share,[fileOwner]=box
usage,[fileDesc]=,[user]=box usage,
[userId]=225282673,[accessTime]=1412700377,[accountName]=box.usage@gmail.com,
[fileId]=21701906465,[fileVersion]=1,[tar-
getHashCode]=da39a3ee5e6b4b0d3255bfef95601890afd80709,[phLogDetail]=
```

```
//the following event is generated when a file called  All Files/share/b.txt was
deleted using the box.usage@gmail.com account
[PH_DEV_MON_BOX_FILE_DELETE]:[eventSeverity]=PHL_INFO,[fileName]=phBoxAgent.cpp,
[lineNumber]=503,[fileType]=file,
[targetName]=b.txt,[fileSize64]=0,[filePath]=/All Files/share,[fileOwner]=box
usage,[fileDesc]=,[user]=box usage,
[userId]=225282673,[accessTime]=0,[accountName]=box.usage@gmail.com,[fileId]-
]=21701844673,[fileVersion]=1,[tar-
getHashCode]=da39a3ee5e6b4b0d3255bfef95601890afd80709,[phLogDetail]=

//the following event is generated when a file called  All Files/share/a.txt was
modified using the box.usage@gmail.com account
[PH_DEV_MON_BOX_FILE_MODIFY]:[eventSeverity]=PHL_INFO,[fileName]=phBoxAgent.cpp,
[lineNumber]=652,[fileType]=file,
[targetName]=a.txt,[fileSize64]=8,[filePath]=/All Files,[fileOwner]=box usage,
[fileDesc]=,[user]=box usage,
[userId]=225282673,[accessTime]=1412700491,[accountName]=box.usage@gmail.com,
[fileId]=21701903189,[fileVersion]=2,[tar-
getHashCode]=0a74245f78b7339ea8cdfc4ac564ed14dc5c22ad,[phLogDetail]=

//the following event is generated periodically for each monitored file and folder
[PH_DEV_MON_BOX_FILE_SHARE]:[eventSeverity]=PHL_INFO,[fileName]=phBoxAgent.cpp,
[lineNumber]=601,[fileType]=folder,
[targetName]=share,[fileSize64]=0,[filePath]=/All Files,[fileOwner]=box usage,
[fileDesc]=,[accountName]=box.usage@gmail.com,
[fileId]=2541809279,[fileVersion]=1,[infoURL]-
]=https://app.box.com/s/zinef627pyuexdcxir1q,[downloadURL]=,[filePass-
wordEnabled]=no,
[filePreviewEnabled]=yes,[fileDownloadEnabled]=yes,[fileUnshareAtTime]=-1,
[filePreviewCount]=0,[fileDownloadCount]=0,[phLogDetail]=
```

Cisco FireAMP Cloud Configuration

- What is Discovered and Monitored
- Configuration
- Sample Events for Salesforce Audit

What is Discovered and Monitored

Protocol	Logs Collected	Used For
CloudAMP API	End point malware activity	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "Cisco FireAMP Cloud" in the **Search** column to see the event types associated with this device.

Rules

There are no predefined rules for Cisco FireAMP Cloud

Reports

There are no predefined reports for Cisco FireAMP Cloud.

Configuration

Create Cisco FireAMP Cloud Credential

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 1, Click **Add** to create a new credential
4. For **Device Type**, select **Cisco FireAMP Cloud**
5. For **Access Protocol**, select **FireAMP Cloud API**
6. For **Password Configuration**, select **Manual** or **CyberArk**
7. For **Manual** credential method, enter **Client ID** and **Client Secret**.
8. **For CyberArk** credential method**,** specify CyberArk properties.
9. Click **Save**.

Test Connectivity

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 2, Click **Add** to create a new association
4. For **Name/IP/IP Range**, enter **api.amp.sourcefire.com**
5. For **Credentials**, enter the name of c redential created in the " Salesforce Audit Credential" step.

6. Click **Save**
7. Select the entry just created and Click **Test Connectivity without Ping.** A pop up will appear and show the Test Connectivity results.
8. Go to **Admin > Setup Wizard > Pull Events** and make sure an entry is created for Microsoft Audit Log Collection

Sample Events for Salesforce Audit

```
[FireAMP_Cloud_Threat_Detected]:[eventSeverity]=PHL_CRITICAL,[con-
nectorGUID]=d2f5d61f-feb0-4b67-80fd-073655b86425,[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,[hostName]-
]=Demo_TeslaCrypt
```

Google Apps Audit Configuration

- What is Discovered and Monitored
- Configuration
- Sample Events for Google Apps 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 **CMDB > Event Types**, search for "Google_Apps" in the **Search** column to see the event types associated with this device.

Rules

There are no predefined rules for Google Apps

Reports

There are many reports defined in **Analytics > Reports > Device > Application > Document Mgmt.** Search for " Google Apps".

Configuration

Create a Google App Credential in Google API Console

1. Logon to Google API Console
2. Under **Dashboard**, create a **Google Apps Project**
   a. **Project Name** - enter a name
   b. Click Create
3. Under **Dashboard**, click **Enable API** to activate Reports API service for this project
4. Create a Service Account Key for this project
   a. Under **Credentials**, click **Create Credentials** > **Create Service Account Key**
   b. Choose **Key type** as JSON
   c. Click **Create**
   d. A JSON file containing the Service Account credentials will be stored in your computer
5. Enable Google Apps **Domain-wide delegation**
   a. Under **IAM & Admin** section, choose the Service account
   b. Check **Enable Google Apps Domain-wide Delegation**
   c. Click Save

6. View Client ID
    a. Under **IAM & Admin** section, choose the Service account
    b. Click **View Client ID**
7. Delegate **domain-wide authority** to the service account created in Step 4
    a. Go to your Google Apps domain's **Admin console**
    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. Select **Manage API Client access** in the Authentication section
    e. In the **Client name** field enter the service account's Client ID (Step 6)
    f. In the **One or More API Scopes** field enter the list of scopes that your application should be granted access to.

Define Google App Credential in FortiSIEM

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 1, Click **Add** to create a new credential.
4. For **Device Type**, select **Google Google Apps.**
5. For **Access Protocol**, select **Google Apps Admin SDK**.
6. Enter the **User Name**.
7. For **Service Account Key**, upload the JSON credential file (Step 4d above)
8. Click **Save**.

Test Connectivity

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 2, Click **Add** to create a new association
4. For **Name/IP/IP Range**, enter **google.com**
5. For **Credentials**, enter the name of c redential created in the " Google App Credential" step.
6. Click **Save**
7. Select the entry just created and Click **Test Connectivity without Ping.** A pop up will appear and show the Test Connectivity results.
8. Go to **Admin > Setup Wizard > Pull Events** and make sure an entry is created for Salesforce Audit Log Collection

Sample Events for Google Apps Audit

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]=8830301951515521023,[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_UY2JDZNp-
gjPKUOF8yJF1A/Nfrg2SFjlC2gR6pJtpP2scVidmc""",Google_Apps_login_login_suc-
cess,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,[act-
or.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.u-
niqueQualifier]=-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,[act-
or.profileId]=117858279951236905887,[event.parameters.ORG_UNIT_NAME]=/test,[id.ap-
plicationName]=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,[act-
or.email]=api1@accelops.net,[event.parameters.NEW_VALUE]=/,[etag]=""6KGrH_UY2JDZNp-
gjPKUOF8yJF1A/r1v9DiPZbL06fXFFjJlrWf2s3qI""",Google_Apps_USER_SETTINGS_MOVE_USER_
TO_ORG_UNIT,MOVE_USER_TO_ORG_UNIT,1,45.79.100.103,,
```

Microsoft Azure AuditTrail Configuration

- What is Discovered and Monitored
- Configuration
- Sample Events for Microsoft Azure Audit Trail

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Azure CLI	None	None	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "Microsoft Azure AuditI" in the **Search** column to see the event types associated with this device.

Rules

There are no predefined rules for Microsoft Azure Audit

Reports

There are no predefined reports for Microsoft Azure Audit.

Configuration

Create Microsoft Azure Audit Credential

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 1, Click **Add** to create a new credential
4. For **Device Type**, select **Microsoft Azure Audit**
5. For **Access Protocol**, select **Azure CLI**
6. For **Password Configuration**, select **Manual** or **CyberArk**
7. For **Manual** credential method, enter the user name and credentials
8. **For CyberArk** credential method**,** specify CyberArk properties.
9. Click **Save**.

Test Connectivity

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 2, Click **Add** to create a new association
4. For **Name/IP/IP Range**, enter some IP Address
5. For **Credentials**, enter the name of c redential created in the " Microsoft Azure Audit Credential" step.
6. Click **Save**

7. Select the entry just created and Click **Test Connectivity without Ping.** A pop up will appear and show the Test Connectivity results.
8. Go to **Admin > Setup Wizard > Pull Events** and make sure an entry is created for Microsoft Audit Log Collection

Sample Events for Microsoft Azure Audit Trail

```
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/re-
sourcegroups/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 Office365 Audit Configuration

- What is Discovered and Monitored
- Configuration
- Sample Events for Google Apps Audit

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
Sway activities	SwayChangeShareLevel, SwayCreate, SwayDelete, SwayDisableDuplication, SwayDuplicate, SwayEdit, EnableDuplication, SwayRevokeShare, SwayShare, SwayExternalSharingOff, SwayExternalSharingOn, SwayServiceOff, SwayServiceOn, SwayView

Office 365 Activity Type	Operation
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 **CMDB > Event Types**, search for "MS_Office365" in the **Search** column to see the event types associated with Office 365.

Rules

There are no predefined rules for Office 365

Reports

There are many reports defined in **Analytics > Reports > Device > Application > Document Mgmt.** Search for "Office365".

Configuration

Create Office365 API Credential

1. Check Office365 Account
    1. Login to Microsoft Online with your Office account
    2. Navigate to office home->admin center->Billing->Purchase services->Office 365 Business Premium
    3. Make sure the you have Office365 Business Premium subscription
2. Create a X.509 certificate and extract some values
    a. Download Windows SDK and install on your workstation
    b. In windows PowerShell run these commands and make sure they succeed

```
PS C:\Program
Files\Microsoft SDKs\Windows\v7.1\Bin> cd "C:\Program
```

```
Files\MicrosoftSDKs\Windows\v7.1\Bin"PS C:\Program
Files\MicrosoftSDKs\Windows\v7.1\Bin> .\makecert.exe -r -pe -n
"CN=Office365Cert"-b 03/15/2016 -e 03/15/2018 -ss FortiSIEM -len 2048
```

c. Open certmgr.msc, and export the new X.509 certificate (office365Cert) by clicking **Action->All Tasks-> Export**
   i. Choose Do not export private key
   ii. Choose Base-64 encoding
   iii. Specify the file name to export

d. Run the following power shell commands to get values $base64Value, $base64Thumbprint, $keyid from the X.509 certificate for use in next step

```
$cer = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("E:\perforce\eng.shg\feature\office365\Office365.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
```

After running these commands, the values will be set as follows

```
(prompt)> $keyid
a8a98039-aa56-4497-ab82-d7c419e70eca
(prompt)> $base64Thumbprint
A7DP44d3q++M+Cq5MQdFZDcwbr4=
(prompt)>$base64Value

MIIC/zCCAeugAwIBAgIQTdQI9aEaZ4FP/zTqmOXZrzAJBgUrDgMCHQUAMBgxFjAUBgNV
BAMTDU9mZmljZTM2NUNlcnQwHhcNMTYwMzE1MDgwMDAwWhcNMTg

wMzE1MDgwMDAwWjAYMRYwFAYDVQQDEw1PZmZpY2UzNjVDZXJ0MIIBIjANBgkqhkiG9w0
BAQEFAAOCAQ8AMIIBCgKCAQEAp9IG5ZNQ9xrtolAc2jUItRhwjm

FKsdST+GTlzax7bXiQl8Zp905DUBgfSyAQr77r/2cDRkf0mV7wW/2i+Pqbfi9CYwzjIN
LyzqxBL5lJPwzVo8aqi/ykILCsbBX6prGvc/TJXjWHbP90AHfZU

t6cDPN3CrE98s3gZlWwz7wDnJP5AU/FXx4Cf4gPZOMEBPRdJqQwIZgLzHk0oDg9kXFoi
wDKORsTiamSMd34nncmmNivrqjKM57pa6jacxWFwbXDov6TlxLm

tniHuH1psMRj/+jkmucoF2c2cRvTdqFePEqoWemB/np7Zwjj6VTruI5Zld22CcNIJY4Z
bheAgYMXmwIDAQABo00wSzBJBgNVHQEEQjBAgBBekE2Kf2vBlJd

fJmP+pAtAoRowGDEWMBQGA1UEAxMNT2ZmaWNlMzY1Q2VydIIQTdQI9aEaZ4FP/zTqmOX
ZrzAJBgUrDgMCHQUAA4IBAQANiw//Vxe04mUInzJUSNXCOUJFj9

HWDzQfbfBOWQQ9YiVm7o0qmSHR8bkaKTxNDl4ng0i6WpMnzmodJjtDpn4I7ZmwAYehBi
FWlUVhAW+M00bvOezcROiscOBuvWd6dQ7Op0XDpYGRnBctCv3w+
```

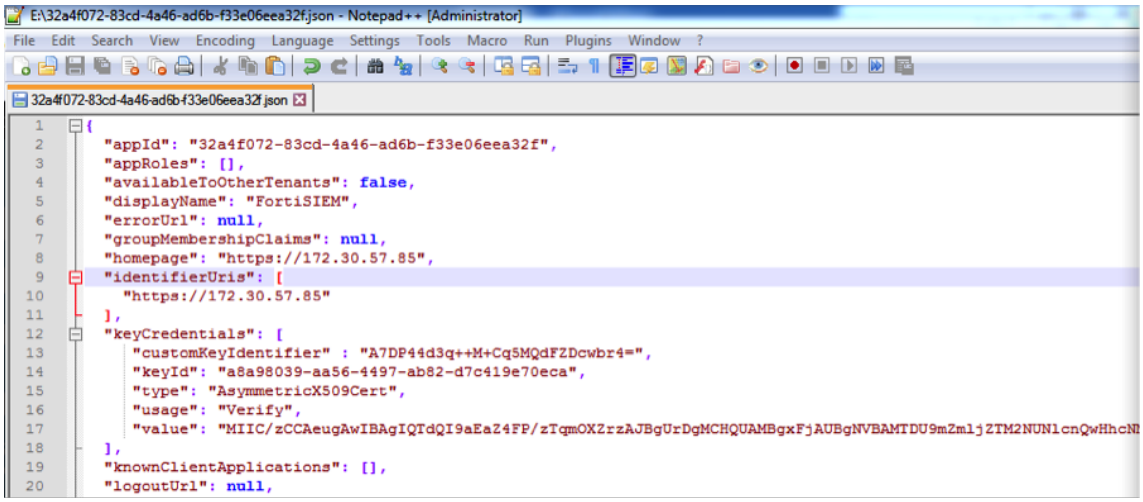
```
YWs0f3odrLCECvO3dk5QJbk500+S8QkLmoVv31/T1BEHnIaY3YudiVO/EpM8n7I/o8Yl
ThHqqSQ6WGeMxYA+ts7yi+Jm++mV6xScK9qWdCbB4BW4ePZWxXi

t5Bod+kC9iSco3o44hmmZdohUpF0t08Gu27dMXsaltd7djb7KeqxZrXihfFC8XeFRBoP
ALIB52Ud
```

3. Create FortiSIEM application in Azure
   a. Login to Azure.
   b. Click **Active Directory** in left panel.
   c. Click **Default Directory** in the right.
   d. Select **APPLICATIONS** tab, then click **ADD**.
   e. Fill application details and click **Next**.
      i. **Name** - FortiSIEM
      ii. **Type** - Choose WEB Application AND/OR API
   f. Fill in **App properties** and **Click Done**
      i. **Sign-on URL** - https://<Supervisor IP>
      ii. **App ID URL** - https://<Supervisor IP>
   g. Click the **application (FortiSIEM)** in left panel, choose Configure tab
      i. **Client ID** is displayed
      ii. **User assignment required** - No
      iii. **Keys** - Select time duration
      iv. **Save**
      v. **Key** is now displayed - copy this key to local workstation. **You would not be able to retrieve it once you leave this page.**
      vi. In the command bar, click **Manage Manifest** and select **Download Manifest**
4. Edit the downloaded JSON file in Step 3.g.vi and
   a. Enter the following in the "keyCredentials" section

```
"customKeyIdentifier" : "$base64Thumbprint_from_above" (Step 2d)
"keyId": "$keyid_from_above", (Step 2d)
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value_from_above" (Step 2d)
```

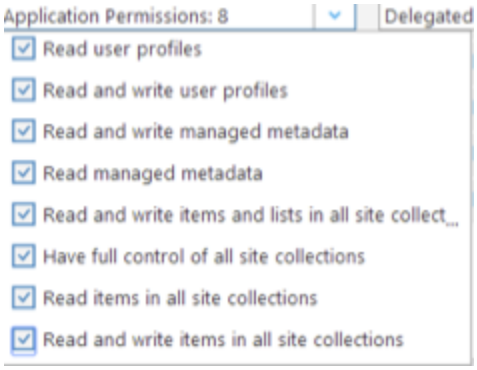
   b. The credential file looks like this.



5. Store the JSON file. Click **Upload Manifest** to upload it to Azure.

Permit Office365 Monitoring

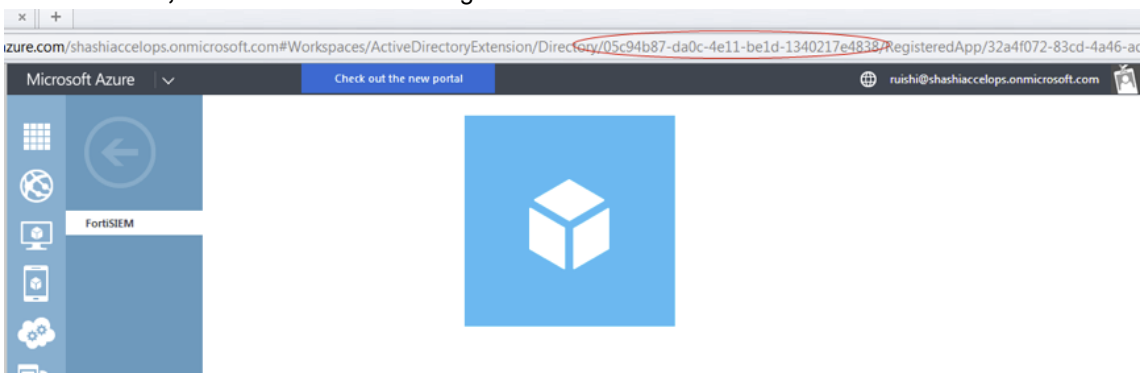
1. Continue with Step 5 above
2. Choose Office 365 Activities
   a. Microsoft 265 Management APIs - Yes
   b. Microsoft Sharepoint Online - Yes
3. Allow read permission to chosen Office365 activities



Define Office365 Management Credential in FortiSIEM

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 1, Click **Add** to create a new credential
   a. For **Name**, provide a name for reference
   b. For **Device Type**, select **Microsoft Office365**
   c. For **Access Protocol**, select **Office365 Mgmt Activity API**

d. **For Tenant ID,** use the ID from Azure Login URL



e. For **Password Configuration**, select **Manual** or

f. For **Client ID**, choose from Step 3.g.i in **Create Office365 API Credential**

g. For **Client Secret**, choose from Step 3.g.v in **Create Office365 API Credential**

4. For **Manual** credential method, enter the user name, password and Security Token.
5. **For CyberArk** credential method**,** specify CyberArk properties.
6. Click **Save**.

Test Connectivity

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 2, Click **Add** to create a new association
4. For **Name/IP/IP Range**, enter **manage.office.com**
5. For **Credentials**, enter the name of c redential created in the **Define Office365 Management Credential** step 3a
6. Click **Save**
7. Select the entry just created and Click **Test Connectivity without Ping.** A pop up will appear and show the Test Connectivity results.
8. Go to **Admin > Setup Wizard > Pull Events** and make sure an entry is created for Office365 Log Collection

Sample Events for Google Apps 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
```

Okta Configuration

FortiSIEM can integrate with Okta as a single-sign 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
- Sample Okta Event

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Okta API			

Event Types

In **CMDB > Event Types**, search for "okta" in the **Device Type** column 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.

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 [act-
ors/0/objectType]=Client [eventId]=tev-UlpTnWJRI2vXNRKTJHE4A1405928963000
[eventName]=USER-AUTH-LOGIN-SUCCESS [published]=2014-07-21T07:49:23.000Z
[requestId]=U8zGA0zxVNXabfCeka9oGAAAA [sessionId]=s024bi4GPUkRaegPXuA1IFEDQ [tar-
gets/0/displayName]=YaXin Hu [targets/0/id]=00uvdkhrxcPNGYWISAGK [tar-
gets/0/login]=YaXin.Hu@accelops.com [targets/0/objectType]=User
```

Salesforce CRM Audit Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "Salesforce Audit" in the **Search** column to see the event types associated with this device.

Rules

There are no predefined rules for Salesforce CRM Audit

Reports

There are many reports defined in **Analytics > 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

Create Salesforce Audit Credential

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 1, Click **Add** to create a new credential
4. For **Device Type**, select **Salesforce Salesforce Audit**
5. For **Access Protocol**, select **Salesforce API**
6. For **Password Configuration**, select **Manual** or **CyberArk**
7. For **Manual** credential method, enter the user name, password and Security Token.
8. **For CyberArk** credential method**,** specify CyberArk properties.
9. Click **Save**.

Test Connectivity

1. Log in to FortiSIEM Supervisor node.
2. Go to **Admin > Setup Wizard > Credentials**.
3. In Step 2, Click **Add** to create a new association
4. For **Name/IP/IP Range**, enter **login.salesforce.com**
5. For **Credentials**, enter the name of c redential created in the " Salesforce Audit Credential" step.
6. Click **Save**
7. Select the entry just created and Click **Test Connectivity without Ping.** A pop up will appear and show the Test Connectivity results.
8. Go to **Admin > Setup Wizard > 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 these console access devices for discovery and monitoring.

- Lantronix SLC Console Manager Configuration

Lantronix SLC Console Manager Configuration

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

Around 10 event types are generated by parsing Lantronix SLC logs. The complete list can be found in CMDB > Event Types by searching for Lantronix-SLC. Some important ones are

- Lantronix-SLC-RunCmd
- Lantronix-SLC-Update
- Lantronix-SLC-User-Logon-Success

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

```
<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 Configuration
- Cisco Security Agent (CSA) Configuration
- ESET NOD32 Anti-Virus Configuration
- FortiClient
- McAfee ePolicy Orchestrator (ePO) Configuration
- Sophos Endpoint Security and Control Configuration
- Symantec Endpoint Protection Configuration
- Trend Micro Intrusion Defense Firewall (IDF) Configuration
- Trend Micro OfficeScan Configuration

Bit9 Security Platform Configuration

- What is Discovered and Monitored
- Bit9 Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "Bit9" in the **Device Type** columns 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 dis-
covered new file 'c:\usersacct\appdata\local\temp\3cziegdd.dll' [361aa7f-
bd5d00aa9952e94adc01d6f8d4cb08766eb03ff522ba5c7a2f9e99f9f]." type="Discovery"
subtype="New file on network" hostname="SVR123" username="SVR123\acct" date-
e="4/6/2015 4:22:52 PM" ip_address="10.168.1.1" pro-
cess="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"
```

Cisco Security Agent (CSA) Configuration

- What is Discovered and Monitored
- Configuration
- SNMP Trap

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Events

There are no specific events defined for this device.

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
```

ESET NOD32 Anti-Virus Configuration

- What is Discovered and Monitored
- ESET NOD32 Configuration

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.

ESET NOD32 Configuration

Syslog

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

- For **Syslog Server,** or the server where the syslogs should be sent, enter the IP address of your FortiSIEM Supervisor.
- 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

```
<35313912>Jul 26 18:06:12 LMHCAPEAV01 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 LMHCAPEAV01 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 'Lmhathnsmt01', 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
- Configuration
- 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 that FortiSIEM collects logs from FortiAnalyzer.

Event Types

In **CMDB** > **Event Types**, search for "FortiClient" 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

1. Configure FortiClient to send events to FortiAnalyzer
2. Configure FortiAnalyzer to send events to FortiSIEM.
   a. Login to FAZ.
   b. Go to **System Settings > Advanced > Syslog Server.**
   c. Click **Create New**.
   d. Set **Name** field - We recommend the name of the FortiSIEM Supervisor node.
   e. Set I**P address (or FQDN)** field to the IP or fully qualified name of the FortiSIEM node that would parse the log (most likely Collector or Worker/Supervisor).
   f. Leave the **Syslog Server Port** to default value 514.
   g. Click **OK** to save your entries.

Sample Events

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""
```

MalwareBytes Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Malware detection log	Security Monitoring

Event Types

In CMDB > Event Types, search for "malwarebytes" to see the event types associated with this device.

Rules

Malware found but not remediated

Reports

In Analytics > Reports, search for "malware found" 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) Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Traps			

Event Types

In **CMDB > Event Types**, search for "mcafee epolicy" in the **Description** column to see the event types associated with this application or device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this device.

Configuration

FortiSIEM processes events via SNMP traps sent by the device.

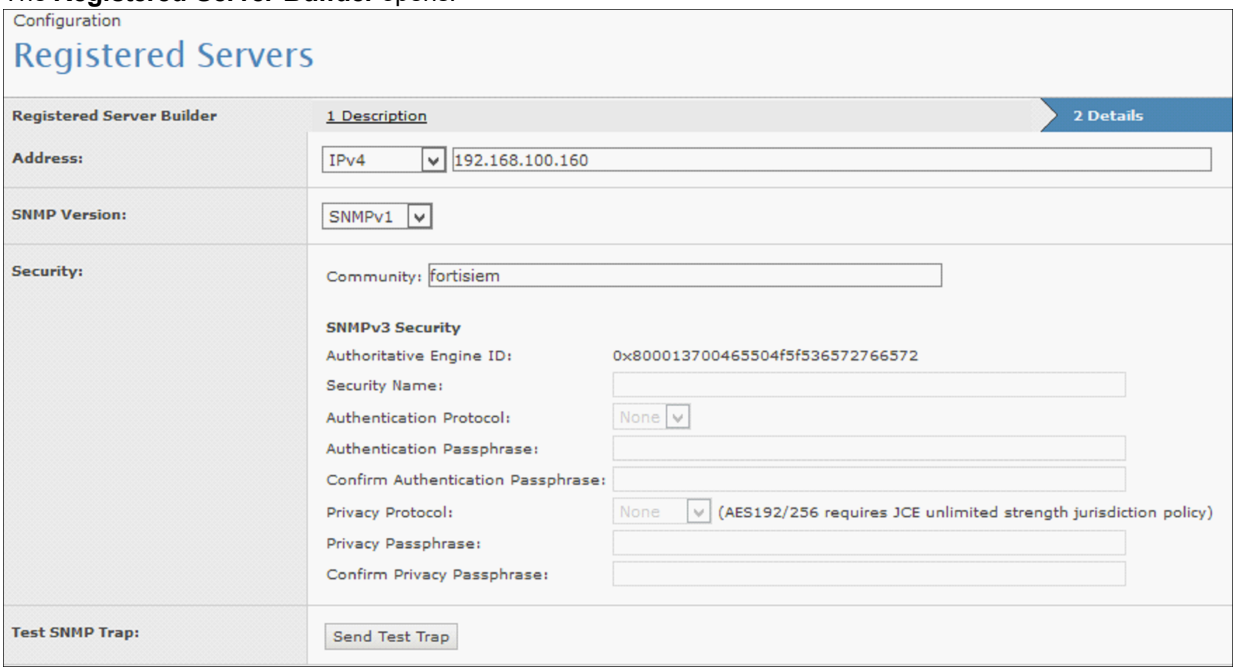
Follow the below procedures to configure McAfee ePO to send Threat based SNMP traps to FortiSIEM.

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.

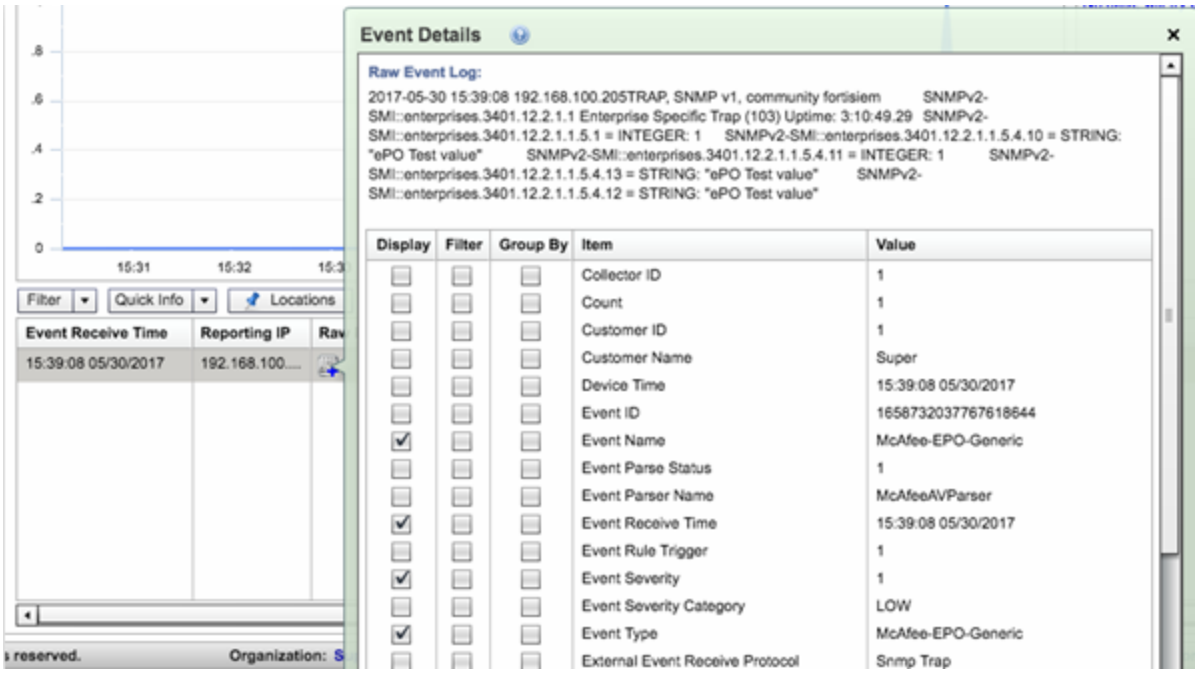
2. Go to **Main Menu > Configuration > Registered Servers**, and click **New Server**.
   The **Registered Server Builder** opens.



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.)



Step 2: Configuring “Automatic Response”

By default, McAfee ePO does not send SNMP Trap alerts for the events that occur. This needs to 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.

Example 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.3401.12.2.1.1.5.2.40 = STRING: "ENDP_AM_1050" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.110 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.410 = STRING: "Access Protection" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.120 = "" 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.3401.12.2.1.1.5.2.100 = STRING: "000c29219964" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.50 = STRING: "McAfee Endpoint
Security"SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.60 = 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.3401.12.2.1.1.5.2.10 = STRING: "05/30/17 13:24:05
UTC" SNMPv2-SMI::enterprises.3401.12.2.1.1.5.2.130 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.150 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.140 = STRING: "192.168.100.205" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.160 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.180 = STRING: "FIREFOX.EXE" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.190 = "" SNMPv2-
SMI::enterprises.3401.12.2.1.1.5.2.170 = STRING: "WIN2012-
SKULLC\Administrator" SNMPv2- SMI::enterprises.3401.12.2.1.1.5.2.400 = 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"
```

Sophos Endpoint Security and Control Configuration

- What is Discovered and Monitored
- Sophos Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

Event Types

In **CMDB > Event Types**, search for "sophos endpoint" in the **Device Type** column to see the event types associated with this application or device.

Rules

There are no predefined rules for this device.

Reports

There are no predefined reports for this 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, com-
munity 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\sys-
tem32\LDPackage.dll\" belongs to virus/spyware 'Mal/Generic-S'."SNMPv2-SMI::en-
terprises.2604.2.1.1.2.2.2 = STRING: "9.5.5"
```

Symantec Endpoint Protection Configuration

- What is Discovered and Monitored
- Symantec Endpoint Protection Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Logs	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "symantec endpoint" in the **Device Type** and **Description** columns 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.

Symantec Endpoint Protection Configuration

Syslog

FortiSIEM processes events from this device via syslogs sent by the device.

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 sjdevswin-
app05,Server: sjdevswinapp05,Domain: Default,Admin: admin,Administrator  log on
failed

<54>Jun 11 12:24:51 SymantecServer sjdevswinapp05: Site: Site sjdevswin-
app05,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:/Docu-
ments and Settings/Administrator.PROSPECTHILLS/Local Set-
tings/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: Glob-
al\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,Oc-
currences: 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,Re-
mote: ,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,Sm-
c,Connected to Symantec Endpoint Protection Manager (10.0.11.17)

<54>Jul 28 08:08:52 SymantecServer corpepp01: 8440p-X0491JYR,Category: 0,Sm-
c,Disconnected from Symantec Endpoint Protection Manager (10.0.11.17)

<54>Jul 28 08:09:52 SymantecServer corpepp01: CORPES-3042,Category: 0,Sm-
c,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,Sm-
c,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 Con-
troller" 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, RetAd-
dr=18005CH",User: afisk,Domain: HST
```

Trend Micro Intrusion Defense Firewall (IDF) Configuration

- What is Discovered and Monitored
- Trend Micro Configuration

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.

Trend Micro Configuration

Syslog

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

- For **Syslog Server,** or the server where the syslogs 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_Autodis-
covery_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 Configuration

- What is Discovered and Monitored
- Trend Micro Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP Trap			

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.

Trend Micro 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 Res-
ult: Virus successfully detected, cannot perform the Clean action (Quarantine) "
```

Environmental Sensors

FortiSIEM supports these devices for monitoring.

- APC Netbotz Environmental Monitor Configuration
- APC UPS Configuration
- Generic UPS Configuration
- Liebert FPC Configuration
- Liebert HVAC Configuration
- Liebert UPS Configuration

APC Netbotz Environmental Monitor Configuration

What is monitored and collected

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 **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	Availability and Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
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 **CMDB > Event Types**, search for "NetBotz" in the **Name** column 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 **Analytics > Rules**, search for "NetBotz" in the **Name** column to see the rules associated with this application or device.

Reports

In **Analytics > Reports**, search for "Netbotz" in the **Name** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

APC UPS Configuration

- 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, 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 **CMDB > Event Types**, search for "apc" in the **Device Type** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "apc" in the **Name** column to see the rules associated with this device.

Reports

In **Analytics > Reports** , search for "apc" in the **Name** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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

Setting Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Generic UPS Configuration

- 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

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

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 the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Liebert FPC Configuration

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

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 **CMDB > Event Types**, search for "LIebert FPC" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "Liebert FPC" in the **Name** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Liebert HVAC Configuration

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

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 - requires the presence of UPS-MIB on the UPS device.

Follow Liebert HVAC documentation to enable FortiSIEM to poll the device via SNMP.

Event Types

In **CMDB > Event Types**, search for "Liebert HVAC" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "Liebert HVAC" in the **Name** column to see the reports associated with this device.

Configuration

SNMP

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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Liebert UPS Configuration

- What is Discovered and Monitored
- Configuration
- Settings for 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

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

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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Firewalls

FortiSIEM supports these firewalls for discovery and monitoring.

- Check Point FireWall-1 Configuration
- Check Point Provider-1 Firewall Configuration
- Check Point VSX Firewall Configuration
- Cisco Adaptive Security Appliance (ASA) Configuration
- Dell SonicWALL Firewall Configuration
- Fortinet FortiGate Firewall Configuration
- Juniper Networks SSG Firewall Configuration
- McAfee Firewall Enterprise (Sidewinder) Configuration
- Palo Alto Firewall Configuration
- WatchGuard Firebox Firewall Configuration

Check Point FireWall-1

- 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, 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

In **CMDB > Event Types**, search for "firewall-1" in the **Device Type** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

LEA

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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Check Point Provider-1 Firewall

- What is Discovered and Monitored
- Configuration Overview

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 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 by following the instructions in Setting Access Credentials for Device Discovery , and then initiate discovery of the device as described in the topics in Discovering Infrastructure .

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall SSLCA Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Check Point Provider-1 Firewall MDS, use these settings. 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 Step 2f above.
    AO Client SIC was generated in Step 2g above
    MDS Server SIC was generated in Step 1 above
    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 need to have configured and discovered 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 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.

Settings for Access Credentials

Settings for Check Point Provider-1 MLM SSLCA Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Check Point MLM over SSLCA, use these settings.

Setting	Value
Name	MLM
Device Type	Checkpoint Provider-1 MLM
Access Protocol	CheckPoint SSLCA
MLM IP	The IPS address of your module

Setting	Value
Checkpoint LEA Port	The port used by LEA on your server
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

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 need to 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 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.

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall CLA SSLCA Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Check Point Provider-1 Firewall CMA, use these settings. 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 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.

Settings for Access Credentials

Settings for Check Point Provider-1 Firewall CLM SSLCA Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Check Point Provider-1 Firewall CMA, use these settings. 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

Check Point VSX Firewall Configuration

- What is Discovered and Monitored
- 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

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 the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

LEA

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 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*.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cisco Adaptive Security Appliance (ASA) Configuration

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

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 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	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
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

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "asa" in the **Device Type** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "asa" in the **Description** column to see the rules associated with this device.

Reports

In **Analytics > Reports**, search for "asa" in the **Description** column to see the reports associated with this device.

Configuration

- Don't Configure SNMP Trap
- Don't configure ASA to send logs via SNMP trap, 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 > Device > Network > Firewall** and select your firewall. Click the **Interface** tab, and make sure that the inside secutity 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).

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>

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

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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 SonicWALL Firewall Configuration

- 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, 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 **CMDB > Event Types**, search for "sonicwall" in the **Device Type** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

- 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 syslogs to FortiSIEM.

Your Dell SonicWALL firewall should now send syslogs 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 pro-
to=tcp/50000
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Fortinet FortiGate Firewall Configuration

- 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, 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

Event Types

In **CMDB > Event Types**, search for "fortigate" in the **Name** and **Description** columns to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "fortigate" in the **Name** column to see the rules associated with this device.

Reports

There are no predefined reports for this device.

Configuration

SNMP and SSH

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.

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.

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
```

Syslog

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
```

Example FortiGate Syslog

```
<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"
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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	<specify device type from drop down>
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

Setting	Value
Device Type	<specify device type from drop down>
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Juniper Networks SSG Firewall Configuration

- 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, 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 **CMDB > Event Types**, search for "SSG" in the **Device Type** column 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

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, refer to sections 'Discovering Infrastructure' and 'Setting Access Credentials' for Device Discovery under Chapter: Configuring FortiSIEM.

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 Syslogs to Send to FortiSIEM

1. Go to **Configuration > Report Setting > Log Settings**.
2. Click **Syslog**.
3. Select the **Severity Levels** of the syslogs 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, Work-
aniser_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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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) Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **CMDB > Event Types**, search for "sidewinder" in the **Device Type** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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-
d=2093,logid=0,cmd=httpp,hostname=wcrfw1.community.int,event="session end",app_
risk=low,
app_categories=infrastructure,netsessid=1adc04dfcb760,src_geo-
o=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
```

Palo Alto Firewall Configuration

- 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, 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 **CMDB > Event Types**, search for "palo alto" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "palo alto" in the **Description** column 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, clickSetup.
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 Policie

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 need to 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 Mesage

```
<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,,,icm-
p,vsys1,untrust,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,Dy-
namicDefault,,,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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Configuration

- What is Discovered and Monitored
- Configuration

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 **CMDB > 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 syslogs 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 syslogs 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-
s="SecureWeb" sub="http" name="http access" action="pass" method="GET" srcip-
p="10.10.10.10" dstip="1.1.1.1" user="" group="" ad_domain="" statuscode="302"
cached="0" profile="REF_DefaultHTTPProfile (Default Web Filter Profile)" fil-
teraction="REF_HttCffCustoConteFilte (Custom_Default content filter action)" size-
e="0" request="0xdc871600" url="http://a.com" referer="http://foo.com/bar/"
error="" authtime="0" dnstime="1" cattime="24080" avscantime="0" fullre-
qtime="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" repu-
tation="unverified" categoryname="Web Ads"
```

WatchGuard Firebox Firewall Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **CMDB > Event Types**, search for "firebox" in the **Device Type** and**Description** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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 Firebox Syslog Message

Spaces in Interface Names

If the interface name has space, for example `outside 0_Interface` instead of `outside0-Interface`, then the string may not be parsed correctly. This is because the log message does not clearly mark the beginning and end of a field.

A clearly specified log format would have specified `"srcIntf = "outside0-Interface""` with a well specified list of keywords such as `srcIntf`, `destIntf`, `srcIpAddr`, etc.

```
<140>Oct 10 17:20:57 server01 (2012-10-10T22:20:57) firewall: Deny 1-Digital out-
side0_Interface 52 tcp 20 63 172.16.7.8 10.12.12.10 34905 22 offset 8 S 3895962691
win 2105 (Everything - Deny-00)
```

Load Balancers and Application Firewalls

FortiSIEM supports these load balancers and application firewalls for discovery and monitoring.

- Brocade ServerIron ADX Configuration
- Citrix Netscaler Application Delivery Controller (ADC) Configuration
- F5 Networks Application Security Manager
- F5 Networks Local Traffic Manager Configuration
- F5 Networks Web Accelerator
- Qualys Web Application Firewall

Brocade ServerIron ADX Configuration

- What is Discovered and Monitored
- Configuration

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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Citrix Netscaler Application Delivery Controller (ADC) Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted and Denied traffic	Log analysis and compliance

Event Types

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "netscaler" in the **Device Type** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "nestler" in the **Name** column to see the reports associated with this device.

Configuration

Syslog

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

- For **Syslog Server,** or the server where the syslogs 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
```

F5 Networks Application Security Manager

- What is Discovered and Monitored
- Configuration

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

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "f5-asm" in the **Name** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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_applic-
ation_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-
p=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 cs6La-
bel=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: applic-
ation/ipp\r\nAccept: application/ipp\r\nUser-Agent: Hewlett-Packard IPP\r\nCon-
tent-Length: 9\r\n\r\n
```

F5 Networks Local Traffic Manager Configuration

- What is Discovered and Monitored
- 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, 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

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "f5-LTM" in the **Name** column to see the event types associated with this device.

Search for "f5-BigIP" in **CMDB > 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

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 the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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, com-
munity 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.3375.2.4.0.1
```

Syslog

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

- For **Syslog Server,** or the server where the syslogs 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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
- Configuration

What is Discovered and Monitored

Protocol	Information discovered	Metrics/Logs collected	Used for
Syslog		Permitted traffic	Log analysis and compliance

Event Types

In **CMDB > Event Types**, search for "f5-web" in the **Name** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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
```

Qualys Web Application Firewall

- What is Discovered and Monitored
- Configuration

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 CMDB > 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.

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-eda5d5b-
b7045","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","cli-
entIp":"172.27.80.170","clientPort":9073,"serverIp":"192.168.60.203","serverPort"

:443},"request":{"method":"POST","uri":"/","protocol":"HTTP/1.1","host":"esers-
test.foo.org","bandwidth":0,"headers":[{"name":"Content-Length","value":"645"},
{"name":"Ac-
cept","-
value":"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;

q=0.8"},{"name":"User-Agent","value":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWe-
bKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36"},{"name":"Con-
tent-Type","value":"application/x-www-form-urlencoded"},
{"name":"Referer","value":"https://esers-test.ohsers.org/"},{"name":"Accept-Encod-
ing","value":"gzip, deflate"},{"name":"Accept-Language","value":"en-US,en;q-
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","c-
at/XPATHi","c-
at/SQLi","qid/150003","loc/req/body/txtUserId","cfg/pol/applicationSecurity"],

"type":"Alert","rule":"main/qrs/sqli/xpathi/condition_escaping/boolean/confidence_
high/3","message":"Condition escaping detected (SQL or XPATH injection) - txtUser-
Id.","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 dis-
abled.","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"}]}}
```

Network Compliance Management Applications

FortiSIEM supports these Network Compliance Management applications and monitoring.

- Cisco Network Compliance Manager Configuration

Cisco Network Compliance Manager Configuration

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 CMDB > 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 Suc-
cessfully 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 Suc-
cessfully 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 con-
figuration via TFTP through CLI Bypassed: deploy to running configuration via SCP
through CLI.  (Requires SCP, CLI to be enabled.) Tried: deploy to running con-
figuration via FTP through CLI (Warning: SSH server username or password not spe-
cified 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 server-
01.foo.com 1.1.1.32  44571 10.173.30.9 $OrignatorEmail$ FooA Update Device Soft-
ware 2014-03-04 03:30:00.0 usmist_1699295009 (1.13.3.9) Succeeded
```

Intrusion Protection Systems (IPS)

FortiSIEM supports these intrusion protection systems for discovery and monitoring.

- AirTight Networks SpectraGuard
- Cisco FireSIGHT
- Cisco Intrusion Protection System Configuration
- Cylance Protect Endpoint Protection
- Cyphort Cortex Endpoint Protection
- FireEye Malware Protection System (MPS)
- IBM Internet Security Series Proventia Configuration
- Juniper DDoS Secure Configuration
- Juniper Networks IDP Series Configuration
- McAfee IntruShield Configuration
- McAfee Stonesoft IPS
- Motorola AirDefense Configuration
- Snort Intrusion Protection System Configuration
- Sourcefire 3D and Defense Center Configuration
- TippingPoint Intrusion Protection System Configuration

AirTight Networks SpectraGuard

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **CMDB > Event Types**, search for "airtight" in the **Device Type** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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

```
<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
```

Cisco FireSIGHT

This section describes how FortiSIEM collects logs from Cisco FireSIGHT console.

- What is Discovered and Monitored
- Configuration

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

- **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

1. Top Cisco FireAMP Malware Events
2. Top Cisco FireAMP File Analysis Events
3. Top Cisco FireAMP Vulnerable Intrusion Events
4. Top Cisco FireAMP Discovered Login Events
5. Top Cisco FireAMP Discovered Network Protocol
6. Top Cisco FireAMP Discovered Client App
7. Top Cisco FireAMP Discovered OS

Configuration

FortiSIEM obtains events from Cisco FireSIGHT via eStreamer protocol.

Cisco FireSIGHT Configuration

1. Logon to Cisco FIRESIGHT console
2. Go to **System** > **Local** > **Registration** > **eStreamer**
3. Click **Create Client**
   a. Enter IP address and password for FortiSIEM
   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

1. Go to **Admin** > **Setup** > **Credentials**
2. Create a credential
    a. Set **Device Type** to Cisco FireAMP
    b. Set **Access Method** to eStreamer
    c. Enter the **Password** as in Step 3a above
    d. Click **Certificate File** > **Upload** and enter the certificate downloaded in Step 5
    e. Click **Save**
3. Create an IP range to Credential Association
    a. Enter **IP address** of the FireSIGHT Console
    b. Enter the **credential** created in Step 2 above
4. Click **Test Connectivity** - FortiSIEM will start collecting events from the FIRESIGHT console.

Cisco Intrusion Protection System Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			Performance and Availability Monitoring
SDEE		Alerts	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "cisco ips" in the **Device Type** and **Description** columns to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "cisco ips" in the **Name** column to see the rules associated with this device.

Reports

In **Analytics > Reports** , search for "cisco ips" in the **Name** column 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 need to create an SDEE account for FortiSIEM to use, go to **Configuration > Users** and **Add** a new administrator.

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>
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cylance Protect Endpoint Protection

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		End point malware alerts	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "cylance" in the **Device Type** column 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.

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
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		End point malware alerts	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "cyphort" in the **Device Type** column 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.

Example Syslog

```
<134>Feb 23 21:58:05 tap54.eng.cyphort.com cyphort: CEF:0|Cy-
phort|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-
e=79ea1163c0844a2d2b6884a31fc32cc4.bin fileType=PE32 executable (GUI) Intel 80386,
for MS Windows startTime=2015-02-24 05:58:05.151123+00
```

FireEye Malware Protection System (MPS)

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **CMDB > Event Types**, search for "fireeye mps" in the **Device Type** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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

```
<164>fenotify-45640.alert: CEF:0|FireEye|MPS|6.0.0.62528|MC|malware-call-
back|9|rt=Apr 16 2012 15:54:41 src=192.168.26.142 spt=0 smac=00:14:f1:90:c8:01 dst-
t=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-
4=https://10.10.10.10/event_stream/events_for_bot?ev_id\=45640 cs5Label=ccName cs5-
5=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
- Configuration

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 CMDB > 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 Rules > Security > Exploits

Reports

There are many reports for this device under 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.

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 FortiSandbox Configuration

- What is Discovered and Monitored
- Configuration

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 CMDB > Event Types, search for "fortisandbox-" to see the event types associated with this device.

Rules

In CMDB > Rules, search for "fortisandbox-" to see the rules associated with this device.

Also, basic availability rules in CMDB > Rules> Availability > Network and performance rules in CMDB > Rules> Performance > Network also trigger

Reports

In CMDB > Reports, search for "fortisandbox-" to see the rules associated with this device.

Configuration

Syslog

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

For Syslog Server, or the server where the syslogs should be sent, enter the IP address of your FortiSIEM virtual appliance.

For Port, enter 514.

Make sure that the syslog format is the same as that shown in the example.

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"
```

IBM Internet Security Series Proventia Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected
SNMP Traps		

Event Types

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "proventia" in the **Device Type** and **Description** column 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

FortiSIEM receives SNMP traps from IBM/ISS Proventia IPS appliances that are sent by IBM/ISS SiteProtector Management Console. You need to 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 andselect **Register withSiteProtector**.
4. Click andselect **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.

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::en-
terprises.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::en-
terprises.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-
Y=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 Aler-
tName: 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"
```

Juniper DDoS Secure Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		DDoS Alerts	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "juniper ddos" in the **Device Type** and **Description** columns 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)
```

Juniper Networks IDP Series Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **CMDB > Event Types**, search for "juniper_idp" in the **Device Type** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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, 'inter-
face=eth3', (NULL), (NULL), (NULL), 0, 0, 0, 0, 0, 0, 0, 0, no, 25, Not
```

McAfee IntruShield Configuration

- What is Discovered and Monitored
- Configuration

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.

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 detec-
ted,AttackTime:2009-03-24 16:23:17 EDT,At-
tackSeverity:Low,SourceIp:127.255.106.236,

SourcePort:N/A,Destin-
ationIp:127.255.106.252,Distin-
ationPort:N/A,AlertId:5260607647261334188,AlertType:Signature,AttackId:

0x00009300,AttackSignature:N/A,
AttackConfidence:N/A,AdminDomain:ASC,SensorName:ASCDCIPS01,Interface:1A-1B,Cat-
egory:Exploit,SubCategory:protocol-violation,Direction:Outbound,
ResultStatus:May be suc-
cessful,DetectionMechanism:signature,ApplicationProtocol:N/A,NetworkProtocol:

N/A,Relevance:N/A,HostIsolationEndTime:N/A
```

McAfee Stonesoft IPS

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Network IPS alerts	Security Monitoring

Event Types

In **CMDB > Event Types**, search for "stonesoft" in the **Device Type** column 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.

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-
p=NTP (UDP) rt=Apr 08 2016 00:26:13 deviceFacility=Inspection act=Allow deviceOut-
boundInterface=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 cs1La-
bel=RuleId cs1=2097152.6
```

Motorola AirDefense Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Wireless IDS logs	Security Monitoring

Event Types

About 37 event types covering various Wireless attack scenarios - search for them by entering "Motorola-AirDefense" in CMDB > EventType.

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 Activ-
ity,CriticalityLevel=Severe,Desc=Rogue AP on Wired Net-
work,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,Cat-
egory=Exploits,CriticalityLevel=Critical,Desc=NAV Attack - CTS,device-
e=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])
```

Snort Intrusion Protection System Configuration

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

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 **CMDB > Event Types**, search for "snort_ips" in the **Device Type** column 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

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 syslogs 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`.

   Modify `alert_syslog` to use a local log facility.
3. **Example for Outputting Syslog to a Local Facility**

   ```
   output alert_syslog: LOG_LOCAL4 LOG_ALERT
   ```
4. Navigate to and open the file `/etc/syslog.conf`.
5. Add a redirector to send syslogs 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 Inform-
ation 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 will need to 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 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.

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]:[eventSever-
ity]=PHL_INFO,[procName]=phAgentManager,[fileName]=AgentSnort,[phLo-
gDetail]=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]:[eventSever-
ity]=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

```
<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,[sensorHost-
name]=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,[dataPay-
load]=302D020101040670756C6963A520...
```

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,[tcpUr-
gentPointer]=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

Settings for Snort IPS over JDBC Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Snort IPS over JDBC, use these settings.

Setting	Value
Name	<database type>-snort-BT
Device Type	Select the type of database that you are connecting to for Snort alerts
Access Protocol	JDBC
Used For	Snort Audit
Pull Interval (minutes)	1
Port	3306

Setting	Value
Database Name	The name of the database
User Name	The administrative user for the Snort database
Password	The password associated with the administrative user

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Sourcefire 3D and Defense Center Configuration

- What is Discovered and Monitored
- Configuration

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog			

Event Types

In **CMDB > Event Types**, search for "sourcefire" in the **Description** column 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 handles SourceFire alerts via syslog either from IPS appliances themselves or from DefenseCenter. Events are classified as Snort event types.

Simply configure SourceFire appliances or DefenseCenter to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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 Syslogs 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/Source-
fireIPS 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 Syslogs from SourceFire DefenseCenter

```
<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 Applic-
ation Attack] [Priority: 1] {tcp} 1.2.3.4:60537->2.3.4.5:80
```

TippingPoint Intrusion Protection System Configuration

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

Instructions - Remove before Publishing

Provide the prefix or keyword to use in searching for events for this application or device in the CMDB. If there are no specific event types for this device, insert this text: There are no event types defined specifically for this device.

In **CMDB > Event Types**, search for "tippingpoint" in the **Device Type** and **Description** columns 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 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 need to 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 Accelops 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 Accelops 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 Accelops virtual appliance appear as an entry in the **Remote Syslogs** table.

Sample parsed syslog messages

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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Routers and Switches

FortiSIEM supports these routers and switches for discovery and monitoring.

- Alcatel TiMOS and AOS Switch Configuration
- Arista Router and Switch Configuration
- Cisco IOS Router and Switch Configuration
- Cisco Meraki Cloud Controller and Network Devices Configuration
- Cisco NX-OS Router and Switch Configuration
- Cisco ONS Configuration
- Dell Force10 Router and Switch Configuration
- Dell NSeries Switch Configuration
- Dell PowerConnect Switch and Router Configuration
- Foundry Networks IronWare Router and Switch Configuration
- HP/3Com ComWare Switch Configuration
- HP ProCurve Switch Configuration
- HP Value Series (19xx) and HP 3Com (29xx) Switch Configuration
- Juniper Networks JunOS Switch Configuration
- Mikrotek Router Configuration
- Nortel ERS and Passport Switch Configuration

Alcatel TiMOS and AOS Switch Configuration

- What is Discovered and Monitored
- 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, 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 **CMDB > Event Types**, search for "alcatel" in the **Device Type** and **Description** columns 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Configuration

- What is Discovered and Monitored
- 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

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.

1. `show startup-config`
2. `show running-config`
3. `show version`
4. `show ip route`
5. `enable`
6. `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 'Discovering Infrastructure' and 'Setting Access Credentials for Device Discovery' under 'Chapter: Configuring FortiSIEM'.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Brocade NetIron CER Routers

- What is Discovered and Monitored
- 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>

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

Cisco 300 Series Routers

- What is Discovered and Monitored
- 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	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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

Setting	Value
Name	<set name>

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

Cisco IOS Router and Switch Configuration

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

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

Protocol	Information Discovered	Metrics collected	Used for
SNMP (V1, V2c, V3)	Hardware component details: serial number, model, manufacturer, software 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, 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

Protocol	Information Discovered	Metrics collected	Used for
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

Protocol	Information Discovered	Metrics collected	Used for
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
Syslog	Device type	System logs and traffic logs matching acl statements	Availability, Security and Compliance

Event Types

Performance Monitoring events

Configuration change events

Syslog events

In **CMDB > Event Types**, search for "cisco_os" in the **Description** column to see the event types associated with this device.

Rules

Performance Monitoring rules

Configuration change rules

Other rules

Reports

Performance Monitoring Reports

Configuration change Reports

Other Reports

Configuration

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.

1. `show startup-config`
2. `show running-config`
3. `show version`
4. `show flash`
5. `show ip route`
6. `show mac-address-table or show mac address-table`
7. `show vlan brief`
8. `show process cpu`
9. `show process mem`
10. `show disk0`
11. `enable`
12. `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.

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-mon-
itor)#type jitter dest-ipaddr <responder ip> dest-port <dest port>ipsla-init(con-
fig-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-mon-
itor)#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,[int-
fName]=Ethernet0/0,[appTransportProto]=snmp,[totFlows]=4752,[recvFlows]=3168,[sen-
tFlows]=1584,[totBytes64]=510127,[recvBytes64]=277614,[sentBytes64]=232513,
[totBitsPerSec]=22528.000000,[recvBitsPerSec]=12288.000000,[sen-
tBitsPerSec]=10240.000000,[phLogDetail]=
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

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 need to 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 Pro-
cessor 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,[hostIpAd-
dr]=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 Configuration

- What is Discovered and Monitored
- 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
SNMP Traps from Cloud Controller		Health	Availability Monitoring

Event Types

- Interface Utilization: PH_DEV_MON_NET_INTF_UTIL

Rules

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

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 the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cisco NX-OS Router and Switch Configuration

- What is Discovered and Monitored
- 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
SNMP (V1, V2c, V3)	OSPF connectivity, neighbors, state, OSPF Area	OSPF state change	Routing Topology, Availability Monitoring

Protocol	Information Discovered	Metrics collected	Used for
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 **CMDB > Event Types**, search for "nx-os" in the **Device Type** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM >

Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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.

1. `show startup-config`
2. `show running-config`
3. `show version`
4. `show flash`
5. `show context`
6. `show ip route`
7. `show cam dynamic`
8. `show mac-address-table`
9. `show mac address-table (for Nexus 1000v)`
10. `show vlan brief`
11. `show process cpu`
12. `show process mem`
13. `show disk0`
14. `enable`
15. `terminal length 0`

Syslog

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

- For **Syslog Server,** or the server where the syslogs 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

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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Setting	Value
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 ONS Configuration

- What is Discovered and Monitored
- 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)	Availability and Performance Monitoring
SNMP Trap		Alerts	Availability and Performance Monitoring

Event Types

Over 1800 event types defined - search for "Cisco-ONS" in **CMDB** > **Event Types**

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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Dell Force10 Router and Switch Configuration

- What is Discovered and Monitored
- 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
Telnet/SSH	Running and Startup configurations	Startup Configuration Change, Difference between Running and Startup configurations	Change monitoring

Event Types

In **CMDB > Event Types**, search for "force10" in the **Description** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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, follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery.

1. `show startup-config`
2. `show running-config`
3. `show version`
4. `show ip route`
5. `enable`
6. `terminal pager 0`

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Dell NSeries Switch Configuration

- What is Discovered and Monitored
- 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

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

Rules

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

- 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Dell PowerConnect Switch and Router Configuration

- What is Discovered and Monitored
- 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
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

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 the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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, follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery.

1. `show startup-config`
2. `show running-config`
3. `show version`
4. `show ip route`
5. `enable`
6. `terminal pager 0`

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Foundry Networks IronWare Router and Switch Configuration

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

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 **CMDB > Event Types**, search for "foundry_ironware" in the **Description** column 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 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 syslogs 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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

HP/3Com ComWare Switch Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "compare" in the **Device Type** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Syslog

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

- For **Syslog Server,** or the server where the syslogs 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 dif-
ferent 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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

HP ProCurve Switch Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "procurve" in the **Device Type** and **Description** columns 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. 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**.

SSH/Telnet

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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

HP Value Series (19xx) and HP 3Com (29xx) Switch Configuration

- What is Discovered and Monitored
- 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

- 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

- 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Juniper Networks JunOS Switch Configuration

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

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

Protocol	Information Discovered	Metrics collected	Used for
Syslog		System logs and traffic logs matching acl statements	Availability, Security and Compliance
sflow		Traffic flow	Availability, Security and Compliance

Event Types

In **CMDB > Event Types**, search for "junos" in the **Device Type** column 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 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 syslogs 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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Mikrotek Router Configuration

- What is Discovered and Monitored
- 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Nortel ERS and Passport Switch Configuration

- What is Discovered and Monitored
- 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Security Gateways

FortiSIEM supports these security gateways for discovery and monitoring.

- Barracuda Networks Spam Firewall Configuration
- Blue Coat Web Proxy Configuration
- Cisco IronPort Mail Gateway Configuration
- Cisco IronPort Web Gateway
- McAfee Web Gateway Configuration
- Microsoft ISA Server Configuration
- Squid Web Proxy Configuration
- Websense Web Filter Configuration

Barracuda Networks Spam Firewall Configuration

- 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, Interfaces, Serial number	CPU utilization, Memory utilization, Interface Utilization	Performance Monitoring
Syslog		Various syslogs - 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 **CMDB > Event Types**, search for "barracuda" in the **Device Type** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Syslog

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

- For **Syslog Server,** or the server where the syslogs 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.k-
world.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 kmc-
gilvrey@qinprop.com - 7 61 - SZ:34602 SUBJ:How FMLA Leave, ADA and Workers' Com-
pensation Work Together April 28, 2011
```

Settings for Access Credentials

Unable to render {include} The included page could not be found.

Blue Coat Web Proxy Configuration

- 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, 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 **CMDB > Event Types**, search for "blue coat" in the **Device Type** and **Description** column 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

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 - - "Shock-
wave 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 need to 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. 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>`.
3. Run `vi /etc/passwd` to change the home directory for `ftpuser` to `/opt/phoenix/cache/bluecoat`. Change only the home directory as shown in this screenshot, 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 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	21
Path	/<Blue Coat IP Address>
Username	bcFtpUser
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       20
06-25 18:13:34 2021 192.168.22.21 200 TCP_TUNNELED 820 1075 CONNECT tcp accel-
ops.webex.com 443 / - - - NONE 172.16.0.141 - - "WebEx Outlook Integration Http
Agent" PROXIED "none" - 25.24.23.22
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cisco IronPort Mail Gateway Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "ironport-mail" in the **Display Name** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports**, search for "ironport mail" in the **Name** and **Description** columns 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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: Mes-
sage 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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cisco IronPort Web Gateway

- What is Discovered and Monitored
- Configuration

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 **CMDB > Event Types**, search for "ironport-web" in the **Display Name** column 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

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

Setting	Value
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://-
fore-
frontdl.microsoft.com/server/scanengineupdate/x86/Kaspersky/Package/1210090007/bases/base1
 - 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};""
```

McAfee Web Gateway Configuration

- What is Discovered and Monitored
- Configuration

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 **CMDB > Event Types**, search for "mcafee_web" in the **Device Type** column 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 syslogs sent by the device. Configure the device to send syslogs to FortiSIEM as directed in the device's product documentation, and FortiSIEM will parse the contents.

- For **Syslog Server,** or the server where the syslogs 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_rol-
lup-
=homepage&page.allowcompete=no&params.styles=fs&Params.User.UserID=4fc6251c068c9f0aa514750
 HTTP/1.1" "Web Ads, Forum/Bulletin Boards" "MinimalRisk" "text/html" 1 "" "" "0"
```

Microsoft ISA Server Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "isa server" in the **Device Type** and**Description** column 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

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

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 will need to use in setting 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 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'.

Syslog

Use the Windows Agent Manager to configure sending syslogs 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 Fire-
fox/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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Squid Web Proxy Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "squid" in the **Description** and **Device Type** columns 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM >

Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Syslog

1. Add this line to the `logformat` section in `/etc/squid/squid.conf`.

```
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
```

2. Add this 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

```
<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.m-
sn.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 Fire-
fox/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
```

Websense Web Filter Configuration

- What is Discovered and Monitored
- Configuration

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 **CMDB > Event Types**, search for "web sense_mail" in the **Display Name** column 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 syslogs sent in the SIEM integration format as described in the Websense SEIM guide. See page 22 for 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_ver-
sion=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
```

Fortinet FortiMail

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

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 CMDB > Event Types, search for "fortimail" to see the event types associated with this device.

Rules

In CMDB > Rules, search for "fortimail" to see the rules associated with this device.

For generic availability rules, see Analytics > Rules > Availability > Network

For generic performance rules, see Analytics > Rules > Performance > Network

Reports

In Analytics > Reports, search for "fortimail" to see the reports associated with this device.

Configuration

Syslog

Configure FortiMail appliance to send logs to FortiSIEM. Make sure the format matches.

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"
```

Fortinet FortiWeb

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

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 CMDB > Event Types, search for "fortiweb" to see the event types associated with this device.

Rules

In Analytics > Rules, search for "fortiweb" to see the rules associated with this device.

For generic availability rules, see Analytics > Rules > Availability > Network

For generic performance rules, see Analytics > Rules > Performance > Network

Reports

In CMDB > Reports, search for "fortiweb" to see the reports associated with this device.

Configuration

Syslog

Configure FortiWenb appliance to send logs to FortiSIEM. Make sure the format matches.

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)
```

Servers

FortiSIEM supports these servers for discovery and monitoring.

- HP UX Server Configuration
- IBM AIX Server Configuration
- IBM OS400 Server Configuration
- Linux Server Configuration
- Microsoft Windows Server Configuration
- Sun Solaris Server Configuration

HP UX Server Configuration

- 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, 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 **CMDB > Event Types**, search for "hp_ux" in the **Description** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "hp_ux" in the **Name** column to see the reports associated with this device.

Configuration

SNMP v1 and v2c

1. Make sure that snmp libraries are installed. Accelops 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 Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Setting	Value
Access Protocol	SSH
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

IBM AIX Server Configuration

- 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, 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 **CMDB > Event Types**, search for "ibm_aix" in the **Device Type** and **Description** column 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

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 Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Setting	Value
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

IBM OS400 Server Configuration

- What is Discovered and Monitored
- Configuration

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 **CMDB > Event Types**, search for "os400" in the **Device Type** column 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 syslogs to FortiSIEM.

Sample Parsed IBM OS400 Syslog Messages

```
Mar 18 17:49:36 ROBINSON CEF :0|PowerTech|Interact|2.0|UNA0603|A File Server trans-
action was allowed for user BRENDAN.|2| src =10.0.1.60 dst =10.0.1.180 msg-
g=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 trans-
action was allowed for user BRENDAN.|2| src =10.0.1.60 dst =10.0.1.180 msg-
g=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 Cli-
ent 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 Configuration

- 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, 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 LinuxFileMon agent)		File or directory change: User, Type of change, directory or file name	Security Monitoring and Compliance

Event Types

In **CMDB > Event Types**, search for "linux" in the **Description** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "linux" in the **Name** column to see the rules associated with this device.

Reports

In **Analytics > Reports** , search for "linux" in the **Name** column to see the reports associated with this device.

Configuration

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 after this please reference net-snmp for further instructions.

Configuring net-smnp-devel

If you havenet-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

FortiSIEM uses the LinuxFileMon monitoring agent to detect user activity and create syslogs. When a change as defined in the configuration file is detected, the agent gets the user information from the Audit module and sends a syslog to FortiSIEM. You will need to install the agent on your Linux server to send syslogs to FortiSIEM.

1. Log in to your server as `root`.
2. Install the audit service.
   This is needed for obtaining user information. For more information about Linux audit files, see this blog post.

```
yum install audit
```

3. Start the audit service.

```
service auditd start
chkconfig auditd on
```

4. Copy the `LinuxFileMon` executable from the FortiSIEM `/opt/phoenix/bin` directory to any location on the server.
   This is the agent that monitors the file changes.
5. Edit the LinuxFileMon configuration file `linuxFileMon.conf` as shown here.
   The file should be in the same directory as the executable.

```
# destIP is the IP address of FortiSIEM and must be the first line
[destIP]=127.0.0.1
# directories or files to monitor - path must be absolute
# Monitored Actions are All, Open, Close, Create, Modify, Delete, Attrib
# Multiple lines must be in different lines
[object]=/tmp/test2/,Open,Delete,Close
[object]=/tmp/test/,All
[object]=/home/bin/LinuxFileMon/test,All
```

6. Start the LinuxFileMon agent.

Sample Parsed Linux Syslog Message

```
Mon Oct 18 16:26:25 2010 PowerEdgeSC440A: [LINUX_FILE_CHANGE|LINUX_FILE_CHANGE]:
[objectType]=Dir,[objectName]=/home/phoenix_dev/-
projects/phoenix/src/cpp/extAgents/linuxFileMon/,[objectAction]=ACCESS,[tar-
getObjType]=File,[targetObjName]="test",[user]=admin
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Configuration

- What is Discovered and Monitored
- Configuration
- Setting Access Credentials

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 that 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**, running processes, open TCP/UDP ports)	Uptime, Overall 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
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	

Protocol	Information Discovered	Metrics collected	Used for
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

Event Types

In **CMDB > Event Types**, search for "windows server" in the **Description** column to see the event types associated with this application or device.

Rules

In **Analytics > Rules**, search for "windows server"in the **Name** column to see the rules associated with this application or device.

Reports

In **Analytics > Reports** , search for "windows server" in the **Name** column to see the reports associated with this application or device.

Configuration

SNMP

Enabling SNMP on Windows Server 2003

SNMP is typically enabled by default on Windows Server 2003, but you will still need to add FortiSIEM to the hosts that are authorized to accept SNMP packets. First you need to 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 will still need to 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

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 will need to use in setting 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 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'.

Syslog

Use the Windows Agent Manager to configure sending syslogs 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. Selet a policy and edit the **Local Security Settings** for the events you want audited. Recommended settings are:

Policy	Description	Settings
Audit account logonevents 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 need to 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.

Setting Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Sun Solaris Server Configuration

- 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, 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 **CMDB > Event Types**, search for "solaris" in the **Device Type** and **Description** column 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

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 Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Setting	Value
Port	22
User Name	A user who has access credentials for your device over SSH
Password	The password for the user

Storage

FortiSIEM supports these storage devices for discovery and monitoring.

- Brocade SAN Switch Configuration
- Dell Compellant Storage Configuration
- Dell EqualLogic Storage Configuration
- EMC Clarion Storage Configuration
- EMC Isilon Storage Configuration
- EMC VNX Storage Configuration
- NetApp Filer Storage Configuration
- Nimble Storage Configuration
- Nutanix Storage Configuration

Brocade SAN Switch Configuration

- 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, 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 **CMDB > Event Types**, search for "brocade" in the **Description** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Dell Compellant Storage Configuration

- 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, 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

- 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Dell EqualLogic Storage Configuration

- 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, 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

Protocol	Information Discovered	Metrics collected	Used for
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 **CMDB > Event Types**, search for "equallogic" in the **Description** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "equallogic" in the **Name** column to see the rules associated with this device.

Reports

In **Analytics > Reports** , search for "equallogic" in the **Name** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

EMC Clarion Storage Configuration

- What is Discovered and Monitored
- Configuration

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 disks** **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 **CMDB > Event Types**, search for "clarion" in the **Name** column 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 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 will need to 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.

Settings for Access Credentials

Settings for EMC Clarion NaviSecCLI Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your EMC Clarion storage device over NaviSecCLI, use these settings.

Setting	Value
Name	EMC Clarion
Device Type	EMC Clarion
Access Protocol	Navisec CLI
User Name	The user you configured to access naviseccli
Password	The password associated with the user

EMC Isilon Storage Configuration

- 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, 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 **CMDB > Event Types**, search for "isilon" in the **Description** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "isilon" in the **Name** column to see the rules associated with this device.

Reports

In **Analytics > Reports** , search for "isilon" in the **Name** column 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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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

Configuring EMC VNX

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) **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

Configuration

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 will need to 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

Settings for EMC VNX NaviSecCLI Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your EMC VNX storage device over NaviSecCLI, use these settings.

Setting	Value
Name	EMC VNX
Device Type	EMC VNX
Access Protocol	Navisec CLI
User Name	The user you configured to access naviseccli
Password	The password associated with the user

NetApp Filer Storage Configuration

- 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, 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

Protocol	Information Discovered	Metrics collected	Used for
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) **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	Performance Monitoring

Protocol	Information Discovered	Metrics collected	Used for
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 **CMDB > Event Types**, search for "netapp" in the **Device Type** column to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "netapp" in the **Name** column to see the rules associated with this device.

Reports

In **Analytics > Reports** , search for "netapp" in the **Name** column 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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Nimble Storage Configuration

- 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, 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 **CMDB > Event Types**, search for "nimble" in the **Description** column 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Nutanix Storage Configuration

- What is Discovered and Monitored
- Configuration

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

Protocol	Information Discovered	Metrics collected	Used for
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, then follow the instructions in Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Virtualization

FortiSIEM supports these virtualization servers for discovery and monitoring.

- HyperV Configuration
- VMware ESX Configuration

HyperV

- What is Discovered and Monitored
- 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 **Analytics** > **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 HyperV performance metrics. Configure this following the guidelines described in Microsoft Windows Server Configuration.

Settings for Access Credentials

Configure WMI on FortiSIEM.

VMware ESX Configuration

- 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

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

When setting the **Access Method Definition** for allowing FortiSIEM to access your <device name> over <protocol>, use these settings.

Setting	Value
Name	vCenter
Device Type	VMware VMware
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 Configuration
- Juniper Networks SSL VPN Gateway Configuration
- Microsoft PPTP VPN Gateway Configuration
- PulseSecure Configuration

Cisco VPN 3000 Gateway Configuration

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

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			
Syslog			

Event Types

In **CMDB > Event Types**, search for "cisco_vpn" in the **Name** and **Device Type** column 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 Messages

```
<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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Juniper Networks SSL VPN Gateway Configuration

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

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
SNMP			
Syslog			

Event Types

In **CMDB > Event Types**, search for "junos_dynamic_vpn" in the **Name** column 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 into your device with administrative credentials.
2. Go to **System > Log/Monitoring > SNMP**.
3. Under **Agent Properties**, enter `public` for **Community**.

Syslog

VPN Access Syslogs

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 Syslogs

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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. 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 Configuration

Configuring Microsoft PPTP

Windows 2003 Server

1. Logon with administrative rights
2. Configure PPTP VPN
    1. 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.
    2. On the Routing and Remote Access wizard, follow the following steps:
        a. Select "Virtual Private Network (VPN) and NAT" and click Next
        b. Select the network interface for use by VPN connection and click Next.
        c. Specify the network that VPN clients should connect to in order to access resources and click Next.
        d. Select VPN IP Address assignment methodology (DHCP/VPN pool) and click Next.
        e. Specify VPN pool if VPN pool was chosen in step d and click Next.
        f. Identify the network that has shared access to the Internet and click Next.
        g. Select if an external RADIUS server is to be used for central authentication and click Next
    3. 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 authen-
tication 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,Con-
nections to Microsoft Routing and Remote Access server,4136,1,4142,0
```

PulseSecure Configuration

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

What is Discovered and Monitored

Protocol	Information Discovered	Metrics Collected	Used For
Syslog		Security and Performance alerts	Security and performance monitoring

Event Types

In **CMDB > 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

Sample PulseSecure Syslog Messages

```
<134> 2015-12-18T06:30:29-08:00  PulseSecure: 2015-12-18 06:30:29 - PAL-B4CDC-
VPNSSL01 - [1.1.1.1] admin(Varian OKTA Realm)[Varian Employees] - Host Checker
policy 'VMS_Host_Checker_Policy' passed on host '1.1.1.1' address ''  for user
'admin'.
```

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Vulnerability Scanners

FortiSIEM supports these vulnerability scanners for discovery and monitoring.

- McAfee Foundstone Vulnerability Scanner Configuration
- Nessus Vulnerability Scanner Configuration
- Qualys Vulnerability Scanner Configuration
- Rapid7 NeXpose Vulnerability Scanner Configuration

McAfee Foundstone Vulnerability Scanner Configuration

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

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 **CMDB > Event Types**, search for "foundstone" in the **Description** column 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 will need to 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

When setting the **Access Method Definition** for allowing FortiSIEM to access your <device name> over <protocol>, use these settings.

Setting	Value
Name	mcafee_jdbc
Device Type	Microsoft SQL Server

Setting	Value
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

Nessus Vulnerability Scanner Configuration

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

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 **CMDB > Event Types**, search for "nessus" in the **Description** and **Device Type** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "nessus" in the **Description** column to see the reports associated with this device.

Configuration

Nessus API

Create a user name and password that FortiSIEM can use as access credentials for the API. 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.

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.

Settings for Access Credentials

Settings for Nessus Vulnerability Scanner API Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your Nessus Vulnerability Scanner over the API, use these settings.

Setting	Value
Name	nessus
Device Type	Nessus Security Scanner
Access Protocol	Nessus API
Pull Interval (minutes)	5
Port	8834
User Name	A user who has permission to access the device over the API
Password	The password associated with the user

Qualys Vulnerability Scanner Configuration

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

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 **CMDB > Event Types**, search for "qualys" in the **Device Type** column to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "qualys" in the **Description** column 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 'Discovering Infrastructure' and 'Setting Access Credentials for Device Discovery' under 'Chapter: Configuring FortiSIEM'.

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

When setting the **Access Method Definition** for allowing FortiSIEM to access your <device name> over <protocol>, use these settings.

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 Configuration

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

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 **CMDB > Event Types**, search for "rapid7" in the **Description** and **Device Type** columns 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**.
   FortiSIEM can only pull reports in this format.

Settings for Access Credentials

Settings for Rapid7 Nexpose API Access Credentials

When setting the **Access Method Definition** for allowing FortiSIEM to access your <device name> over <protocol>, use these settings.

Setting	Value
Name	rapid7
Device Type	Rapid7 NeXpose Vulnerability Scanner
Access Protocol	Rapid7 NeXpose API
Pull Interval (minutes)	5
Port	3780
User Name	A user who can access the device over the API
Password	The password associated with the user

WAN Accelerators

FortiSIEM supports these wide area network accelerators for discovery and monitoring.

- Cisco Wide Area Application Server Configuration
- Riverbed SteelHead WAN Accelerator Configuration

Cisco Wide Area Application Server Configuration

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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

Riverbed SteelHead WAN Accelerator Configuration

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

Protocol	Information Discovered	Metrics collected	Used for
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. Around 115 traps defined in CMDB > Event Types. The mapped event types start with "Riverbed-".	Availability, Security and Compliance

Event Types

In **CMDB > Event Types**, search for "steelhead" in the **Description** and **Device Type** columns to see the event types associated with this device.

Rules

In **Analytics > Rules**, search for "steelhead" in the **Name** column to see the rules associated with 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, then follow the instructions in the User Guide > Section: Configuring FortiSIEM > Discovering Infrastructure > Setting Access Credentials for Device Discovery to establish the connection between the device and FortiSIEM, and to initiate the device discovery process.

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

Settings for Access Credentials

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Wireless LANs

FortiSIEM supports these wireless local area network devices for discovery and monitoring.

- Aruba Networks Wireless LAN Configuration
- Cisco Wireless LAN Configuration
- FortiAP
- FortiWLC
- Motorola WiNG WLAN AP Configuration
- Ruckus Wireless LAN Configuration

Aruba Networks Wireless LAN Configuration

- What is Discovered and Monitored
- 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 **CMDB > Event Types**, search for "aruba" in the **Description** and **Device Type** columns to see the event types associated with this device.

Rules

There are no predefined rules for this device.

Reports

In **Analytics > Reports** , search for "aruba" in the **Name** column 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

SNMP Access Credentials for All Devices

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

Cisco Wireless LAN Configuration

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 **CMDB > Event Types**, search for "cisco wireless" in the **Description** column 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, com-
munity 1n3t3ng . Cold Start Trap (0) Uptime: 0:00:00.00 DISMAN-EVENT-
MIB::sysUpTimeInstance = Timeticks: (9165100) 1 day, 1:27:31.00 SNMPv2-MIB::s-
nmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.9.9.599.0.4 SNMPv2-SMI::en-
terprises.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::en-
terprises.9.9.599.1.3.1.1.8.0 = Hex-STRING: 00 25 45 B7  66 70  SNMPv2-SMI::en-
terprises.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::en-
terprises.9.9.599.1.2.1.0 = STRING: "IE\brouse" SNMPv2-SMI::en-
terprises.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::en-
terprises.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::en-
terprises.9.9.513.1.1.1.1.5.0 = STRING: "AP03-3.rdu2" SNMPv2-SMI::en-
terprises.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::en-
terprises.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::en-
terprises.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" SNMPv2-SMI::en-
terprises.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::en-
terprises.9.9.615.1.2.10.0 = STRING: "-83,-85" SNMPv2-SMI::en-
terprises.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

When setting the **Access Method Definition** for allowing FortiSIEM to communicate with your device over SNMP, use these settings. Set the **Name** and **Community String**.

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

FortiAP

- What is Discovered and Monitored
- Configuration
- Sample events

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 **CMDB** > **Event Types**, search for "FortiGate-Wireless" and “FortiGate-event” in the Description column 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]=
```

FortiWLC

- What is Discovered and Monitored
- Configuration
- 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 **CMDB > Event Types**, search for "FortiWLC" in the **Description** column 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 FortiWLC to:

a. Send Syslog to FortiSIEM.
b. Enable SNMP read from FortiSIEM.

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 Configuration

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 **CMDB > 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
```

Ruckus Wireless LAN Configuration

- What is Discovered and Monitored
- Configuration

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.

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 will need to 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 need to 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 needs to be enabled and certificates need to be defined.

The following configurations are already added to phoenix_config.txt in Super/Worker and Collector nodes.

```
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
```

Note - the syslog over TLS client needs to be configured to communicate properly with FortiSIEM.

Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.