

Enterasys SIEM Supported Devices List (DSMs)

Enterasys SIEM (also known as DSCC) collects security events from a heterogeneous set of sources that includes network infrastructure, security devices, servers, and applications. It normalizes all events to enable automatic out-of-the-box correlation with other events and network flows. In addition, Enterasys SIEM surveys the entire network, using native flow sources in a customer's routing/switching infrastructure or data from distributed collectors to gather a detailed history of all network flow activity. Enterasys SIEM supports the following industry-flow formats.

NetFlow
J-Flow
SFlow
cFlowd
Packeteer Flow Data Record

Enterasys SIEM Supported Devices/Event Sources

Manufacturer	Device Name	Device Type
3Com	8800 Series Switch	Router
Apache	HTTP Server	Web Server
Apple	OS X	Operating System
Array Network	ArraySP	SSL VPN
Aruba Networks	Mobility Controllers	Wireless Management
BlueCoat	Blucoat SG	Proxy Server
Bridgewater	AAA Service Controller	Authentication
Check Point	FireWall-1	Firewall
Check Point	Provider-1	Management
Check Point	VPN-1	VPN
Cisco	ACS	AAA Server
Cisco	Aironet	Access Point
Cisco	Catalyst Switch	Switch
Cisco	NAC Appliance	NAC
Cisco	PIX Firewall	Firewall
Cisco	Router IOS	Router
Cisco	VPN 3000 Concentrator	VPN
Cisco	ASA	VPN/Security
Cisco	CatOS	Switches
Cisco	FWSM	Firewall Support Module
Cisco	IPS	IDS
Cisco	Security Agent (CSA)	Host based Agent
Cisco	Wireless Services Module (WiSM)	Management
Crypto-Card	Crypto-Shield	Security Appliance
eEye REM Security Management Console and the Network Security Scanner	eEye	VA Scanner
Enterasys	Dragon	IDS
Enterasys	Hi Guard	Wireless IPS
Enterasys	Hi Path	Wireless
Enterasys	NetSight ASM	Security Management
Enterasys	Matrix Router	Router
Enterasys	Secure Stack	Switch
Enterasys	XSR	Router
Extreme Networks	ExtremeWare	Router
F5 Networks	BigIP	Load Balancer
ForeScout	CounterACT	IPS Security Appliance
FortiNet	FortiGate	IDS
Foundry	Switch / Router	Switch
Foundstone	FoundScan	VA Scanner

Enterasys SIEM Supported Devices/Event Sources

Manufacturer	Device Name	Device Type
Generic	Authentication Server	Authentication
Generic	Firewall	Firewall
HP	Tandem NonStop	OS
HP	UX	OS
IBM	AIX 5L	OS
IBM	Lotus Notes Domino	Application
IBM	Proventia Server	Intrusion Prevention
IBM	zOS Mainframe RACF	OS
IBM	Site Protector Server	Intrusion Prevention
IBM	Websphere	
ICSA	BIND	application
Imperva	SecureSphere	Database Security
Jflow	Juniper Routers	Flow Source
Juniper	AVT	
Juniper	DX Application Acceleration Platform	Security Appliance
Juniper	EX Series Switch	Switch
Juniper	Infranet Controller (IC)	Security Appliance
Juniper	ISG	Integrated Security Gateway
Juniper	NetScreen Firewall	Firewall
Juniper	NetScreen IDP	Intrusion Prevention
Juniper	NSM	NetScreen Security Manager
Juniper	Profiler	VA Scanner
Juniper	RA/SA Series SSL VPN	SSL VPN
Juniper	Router	Router
Juniper	SRX	Router
Juniper	SSG	Secure Services Gateway
Juniper	Steel Belted Radius	AAA Server
Linux	DHCP Server	DHCP Server
Linux	Iptables kernel 2.4 and above	Firewall
	Open Source Linux Login/ Logout Log	
Linux (includes Red Hat)	Red Hat Login/ Logout	Operating System
McAfee	ePolicy Orchestrator	AV
McAfee	Intrushield	Intrusion Prevention
MetalInfo	MetalP	DHCP Server
Microsoft	Authentication (Windows Event Log)	Operating System
Microsoft	DHCP Server	DHCP Server
Microsoft	Exchange Server	Email Server
Microsoft	IAS	Authentication
Microsoft	IIS	Web Server
Microsoft	SQL Server	Database
Microsoft	Windows	Operating System
Motorola/Symbol	Access Point (AP)	wireless AP
nCircle	IP-360	VA Scanner
Nessus	Scanner	VA Scanner
NetFlow	Any devices that supports NetFlow	Flow Source
Niksun	NetVCR 2005	IDS
NMAP	Scanner	VA Scanner
Nokia	Firewall	Firewall/VPN
Nokia	IP Series	Firewall/VPN
Nortel	Application Switch (NAS)	Application Switch
Nortel	ARN (BayRS)	Router
	Ethernet Routing Switch (ERS) 2500, 4500, 5500	Router
Nortel	Ethernet Routing Switch (ERS) 8300/8600	Router
Nortel	Secure Router (SR)	Router
Nortel	Switched Firewall 5100/6000	FW

Enterasys SIEM Supported Devices/Event Sources

Manufacturer	Device Name	Device Type
Nortel	Threat Protection System (TPS) Intrusion Sensor (IS)	IDS
Nortel	VPN Gateway	VPN
Nortel	VPN Router	VPN
Nortel	VPN Router (Contivity VPN Switch)	VPN
Oracle	Database	Database
Oracle	DB Listener	Database Security
Packeteer FDR	PacketShaper	FDR
Patchlink	VIS	VA Scanner
ProFTP	ProFTP	FTP Server
Qualys	QualysGuard	VA Scanner
Rapid7	NeXpose	VA Scanner
Redback		Router/Switch
RSA	Authentication Manager	Authentication
Samhain Labs	Samhain HIDS	Host IDS
SAP	R3	Enterprise Application
Secure Computing	Cyberguard	FW/VPN
Secure Computing	SideWinder G2	Security Appliance
Sentriigo	Hedgehog	Security Appliance
Sflow	Foundry	Flow Source
Snort	Intrusion Detection System (IDS)	IDS
SonicWall	UTM/Firewall/VPM Appliance	Firewall
SourceFire	Intrusion Sensor	IDS
Squid	Web Proxy	Proxy Server
Starent Networks	Carrier class switch Mgmt.	Switch Manager
Sun	Sendmail	Mail Server
Sun	Solaris (Login/logout Log)	Operating System
Sun	Solaris DHCP	DHCP Server
Sybase	ASE	Database
Symantec	Endpoint Protection	Endpoint Protection
Symantec	SGS Appliance	Firewall
Symantec	System Center (SSC)	Anti-Virus Management Console
Symantec	Anti-Virus Client	Anti-Virus client
Symark	Power Broker	OS Command Proxy
HP	Tandem NonStop	OS
Tipping Point	Intrusion Prevention System (IPS)	Intrusion Prevention
Tipping Point	SMS (multi-sesnor management)	Management
Tipping Point	X Series Appliances	IPS
Top Layer	IPS 5500	IPS
Trend Micro	InterScan VirusWall	Anti-Virus
Trend Micro	OfficeScan	Anti-Virus
Trend Micro	Control Manager	Management
Tripwire	Enterprise/Manager	Software
TrustWave	IPAngel	IDS
Universal	Syslog, SDEE, and SNMP	Generic
Vericept	Content 360	Security Appliance

Enterasys SIEM Supported Devices/Event Sources		
Manufacturer	Device Name	Device Type
Supported DSM Extensions		
Aladdin	eSafe	
Alcatel-Lucent	VitalQIP	
Astaro	Security Gateway	UTM Appliance
Aventail	EX-2500 VPN	
Checkpoint	Endpoint Security	Desktop Security
Cisco	ASA (VPN Identity Parsing)	
DD-WRT	Linux wireless router firmware	OS
DeepNines	iTrust	
eLitecore	Cyberoam	
ISC	Bind	Name Server
Linux	IPTables	Firewall
Microsoft	ISA	Proxy
Mirapoint	Message Server	Messaging
NetApp	3020, 6040	
Network RADIUS	FreeRADIUS	
Nortel	IDEngines	
OpenBSD	FTP Daemon	OS
PaloAlto Networks	PA Series	network switch
Reflex	IPS	IPS
Riverbed	Steelhead	
SAP	ERP	Enterprise Application
Sun	LDAP	Directory Server
Shrubbery Networks	TACACS+ Daemon	Authentication
Watchguard	Firebox	firewall

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**,
or +1-978-684-1000 and visit us on the Web at enterasys.com



©2009 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.



Delivering on our promises. On-time. On-budget.