

TAP SUPPORTED DEVICES

AUTHORITATIVE LIST: VERSION 18, MARCH 2017

AUTHOR: RHIANNON HARGRAVE




	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
1	Adallom	Applications	Application Security	syslog	✓	adallom
2	AdTran	Firewall	NetVanta	syslog		adtran_netvanta
3	Aerohive	Network Access Points	Access Point	syslog		aerohive_ap
4	Airtight	Network Access Points	Access Point	syslog		airtight_ap
5	Amazon Web Services	Web Content	CloudTrail	syslog		aws_cloudtrail
6	Amazon Web Services	Web Content	CloudFront	syslog		aws_cloudfront
7	Amazon Web Services	Web Content	Simple Storage Service (S3)	syslog		aws_s3
8	Amazon Web Services	Web Content	Elastic Load Balancing (ELB)	syslog		aws_elb
9	Amazon Web Services	Web Content	Virtual Private Cloud	syslog		aws_vpc_flow
10	Apache	Applications/ Host / Server / Web Content / Filtering / Proxies	HTTP Server	syslog		apache_http_server
11	Apache	Applications	TomCat	syslog		apache_tomcat
12	Apache	Applications / Firewalls	ModSecurity	syslog		apache_modsecurity
13	Apache	Applications	Cassandra	syslog		apache_cassandra
14	APC	Other	UPS	syslog		apc_ups

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
15	Aruba Networks	Network Switches & Routers	Aruba OS	syslog		aruba_networks
16	Balabit	Application	Syslog-NG	syslog		balabit_syslogng
17	Barracuda	Firewalls	Next Generation Firewall	syslog		barracuda_ngfw
18	Barracuda	VPN	SSL VPN	syslog		barracuda_sslvpn
19	Barracuda	Firewalls	Web Application Firewall	syslog		barracuda_waf
20	BeyondTrust	Applications	BeyondInsight	syslog	✓	beyondtrust_beyondinsigh
21	Blue Coat Systems	Applications/ Host / Server / Web Content / Filtering / Proxies	WebFilter	syslog		bluecoat_http_proxy
22	Blue Coat Systems	Web Content / Filtering / Proxies	ProxySG	syslog		bluecoat_ops
23	Blue Coat Systems	Security Mangement	Content Analysis	syslog		bluecoat_ops
24	Blue Coat Systems	Antivirus / Malware	Malware Analysis	syslog		bluecoat_ops
25	Bradford Networks	NAC / Network Switches & Routers	Network Sentry/NAC	syslog	✓	bradford_network_security

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
26	Bro	IPS / IDS	Network Security Monitor	syslog		bro_conn, bro_dhcp, bro_dnp3, bro_dns, bro_dpd, bro_files, bro_ftp, bro_http, bro_intel, bro_irc, bro_kerberos, bro_known_certs, bro_known_hosts, bro_known_services, bro_loaded_scripts, bro_modbus, bro_mysql, bro_notice, bro_packet_filter, bro_pe, bro_radius, bro_rdp, bro_smb_auth, bro_smb_cmd, bro_smb_mapping, bro_smtp, bro_smtp_entities, bro_smtpurl, bro_snmp, bro_software, bro_ssh, bro_ssl, bro_syslog, bro_tunnels, bro_weird, bro_x509
27	Brocade	NAC / Network Switches & Routers	Vyatta VRouter	syslog		brocade_vyatta_vrouter
28	Bromium	Application	vSentry Endpoint Monitoring	syslog		bromium_vsentry
29	Carbon Black	Endpoint Security	Endpoint Security Platform	syslog		carbonblack_er
30	Centrify	Authentication	Server Suite	syslog		centrify_suite
31	Checkpoint	Firewall	Firewall	syslog		checkpoint_firewall
32	Checkpoint	Web Content / Filtering / Proxies	HTTP Proxy	syslog		checkpoint_http_proxy
33	Checkpoint	Firewall	NG Firewall	syslog		checkpoint_ng_firewall

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
34	Checkpoint	IPS / IDS	SmartDefense	syslog		checkpoint_smartdefense
35	Cisco	NAC / Network Switches & Routers	Access Control System (ACS)	syslog		cisco_acs
36	Cisco	Firewall / VPN / HA / Routing	Adaptive Security Appliance (ASA)	syslog		cisco_asa, cisco_asa_cws cisco_asa_threat_detectio cisco_firepower_ips
37	Cisco	Web Content / Filtering / Proxies	Adaptive Security Appliance Cloud Web Services (ScanSafe)	syslog		cisco_asa_cws
38	Cisco	Firewall	Firewall Services Module (FWSM)	syslog		cisco_fwsm, cisco_fwsm_threat_detecti
39	Cisco	Network Switches & Routers	HSRP	syslog		cisco_hsrp
40	Cisco	IDS	Intrusion Detection System	syslog		cisco_ids
41	Cisco	Network Operating Systems	IOS	syslog		cisco_ios
42	Cisco	IPS	IPS	syslog		cisco_ips
43	Cisco	Applications/ Host / Server / Web Content / Filtering / Proxies	Web Security (IronPort)	syslog		cisco_ironport_http_proxy
44	Cisco	Application Control / IPS / Firewall / Email	Email Security (IronPort)	syslog		cisco_ironport_email


	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
45	Cisco	Authentication	Identity Services Engine	syslog		cisco_ise
46	Cisco	Network Switches & Routers	Nexus	syslog		cisco_nexus
47	Cisco	NAT / Firewall	Private Internet Exchange (PIX)	syslog		cisco_pix, cisco_pix_threat_detection
48	Cisco	Web Content	VCS	syslog		cisco_vcs
49	Cisco	IP Telephony	VOIP	syslog		cisco_voip
50	Cisco	Virtual Private Networks	VPN	syslog		cisco_vpn
51	Cisco	Network	WLC	syslog		cisco_wlc
52	Citrix	Application	Independent Management Architecture (IMA)	syslog		citrix_ima
53	Citrix	Application	Netscaler	syslog		citrix_netscaler
54	Cloudlock	Application	API	syslog		cloudlock_api
55	Code Green Networks	Application	DLP	syslog		codegreen_dlp
56	Collectd	Application	collectd	syslog		collectd
57	CyberArk	Application	Privileged Threat Analytics (PTA)	syslog		cyberark_pta
58	CyberArk	Application	Enterprise Password Vault	CEF		cyberark_vault
59	Darktrace	Application	DCIP	syslog /CEF		darktrace_dcip

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
60	Dovecot	Email Security	Email	syslog		dovecot_email
61	Duo	Authentication	Authentication	syslog		duo_auth
62	ESET	Remote Administration	Remote Admin Server	syslog		eset_raserver
63	eStreamer	Application	eStreamer	syslog		estreamer
64	ExtraHop	Application	SSH, Database, HTTP, Storage	syslog		extrahop
65	F5	Applications/ Host / Server / Web Content / Filtering / Proxies	BIG-IP Application Security Manager (ASM)	syslog		f5, f5_asm
66	F5	Applications/ Host / Server / Web Content / Filtering / Proxies / NAC	BIG-IP Access Policy Manager (APM)	syslog		f5_bigip_apm
67	F5	Application	BIG-IP Threat Management Microkernel (TMM)	syslog		f5_bigip_tmm
68	FairWarning	Application	Patient Privacy Monitoring	syslog		fariwarning_ppm
69	Fidelis	Application	Advanced Threat Detection, Network Analytics	syslog		fidelis_systems
70	FireEye	Applications/ Host / Server / Web Content / Filtering / Proxies	Web Security	syslog		fireeye

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
71	FireEye	Email Security	Email Security	syslog		fireeye_ex, fireeye_etp
72	FireEye	Content Security	Content Security	syslog		fireeye_cms
73	FireEye	Host / Application Security	Endpoint Security	syslog		fireeye_nx, fireeye_hx
74	ForeScout	NAC / Network Switches & Routers	Network Access Control (NAC)	syslog	✓	forescout_counteract, forescout_nac
75	Forgerock	Web Policy	Tomcat	syslog	✓	forgerock_tomcat
76	Fortinet	Applications / Host Server / Web Content / Proxies	Fortigate	syslog		fortinet_fortigate
77	HP	Security Mangement	ArcSight	syslog, CEF		(vendor specific)
78	HP	IPS / IDS	TippingPoint	syslog		tipping_point_ips
79	IBM	Mainframe Operating System	OS 390	syslog		ibm_os_390
80	IBM	IPS/IDS	Proventia	syslog		ibm_proventia
81	Imperva	Applications / Web Content / Firewalls	SecureSphere WAF	syslog		imperva_securesphere_wa
82	Infoblox	Other	Trinzic Network Services (DHCP, DNS)	syslog		dhcpd_dhcp, bind_dns
83	ISC	DNS Server	Bind9	syslog		bind_dns
84	ISC	DHCP Server	dhclient	syslog		dhclient_dhcp
85	Jasig	Authentication	Central Authentication Service (CAS)	syslog		jasig_cas


	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
86	Juniper	Network Switches & Routers	Routers (rt_flow)	syslog		juniper_flow
87	Juniper	Network Switches & Routers	SRX Services Gateway (SSG)	syslog		juniper_flow
88	Juniper	Virtual Private Networks	VPN	syslog		juniper_vpn
89	Juniper	Network Operating Systems	JunOS	syslog		juniper_ops
90	Juniper	Firewall/VPN	Netscreen	syslog		juniper_netscreen
91	Lucent	Firewalls	Firewall	syslog		lucent_firewall, lucent_fw
92	Lumension	Antivirus / Malware	Endpoint Management and Security Suite: Antivirus	syslog		lumension_detection_agen
93	Mandiant	Security Management	Mandiant Intelligent Response (MIR)	syslog		mandiant_mir
94	Mandiant	Security Management	Mandiant for Security Operations (MSO)	syslog		mandiant_mso
95	McAfee	Security Management	ePO (ePolicy)	syslog		mcafee_epolicy
96	McAfee	IPS / IDS	Host Intrusion Prevention Server	syslog		mcafee_intrushield, mcafee_ips
97	Microsoft	DNS Server	DNS Server	syslog		ms_dns
98	Microsoft	DHCP Server	DHCP Server	syslog		ms_dhcp



	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
99	Microsoft	Email Security	Exchange Server	syslog		ms_exchange
100	Microsoft	Applications/ Host / Server / Web Content / Filtering / Proxies	Internet Information Services (IIS)	syslog		ms_iis
101	Microsoft	Other	Event	syslog		ms_windows_event, ms_windows_security, ms_windows_perfmon
102	Microsoft	Network Monitoring	Systems Center Operations Manager (SCOM)	syslog		ms_scom
103	Microsoft	Network Monitoring / Firewall	Threat Management Gateway (TMG) Firewall	syslog		ms_tmg_firewall
104	Microsoft	Web Content / Filtering / Proxies	Threat Management Gateway (TMG) HTTP Proxy	syslog		ms_tmg_http_proxy
105	Microsoft	Firewall, Web Content / Proxies	Threat Management Gateway	syslog		ms_tmg_firewall, ms_tmg_http_proxy
106	Nagios	Network Monitoring	Nagios Core	syslog		nagios
107	Nginx	Web Content / Filtering / Proxies	HTTP Proxy	syslog		nginx
108	Nortel	Virtual Private Networks	VPN	syslog		nortel_vpn
109	OCLC	Proxies	EZProxy	syslog		oclc_ezproxy

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
110	Oracle	Application / Security	Audit	syslog		oracle
111	Palo Alto	Firewall	PA Series Firewalls	syslog		paloalto_firewall, paloalto_http_proxy, paloalto_system, paloalto_threat_data, paloalto_threat_file, paloalto_threat_flood, paloalto_threat_scan, paloalto_threat_spyware, paloalto_threat_url, paloalto_threat_virus, paloalto_threat_vulnerabili paloalto_threat_wildfire, paloalto_traffic, paloalto_correlation
112	Palo Alto	Firewall / Security Mangement	Next Generation Enterprise Security Platform	syslog		paloalto_firewall, paloalto_http_proxy, paloalto_system, paloalto_threat_data, paloalto_threat_file, paloalto_threat_flood, paloalto_threat_scan, paloalto_threat_spyware, paloalto_threat_url, paloalto_threat_virus, paloalto_threat_vulnerabili paloalto_threat_wildfire, paloalto_traffic, paloalto_correlation
113	Postfix	Email Server	Email Server	syslog		postfix_mail_ta
114	ProofPoint	Email Server	Sendmail	syslog		proofpoint_sendmail
115	Puppet Labs	Application	Puppet Console	syslog		puppet
116	QOS	Applications	LogBack	syslog		logback
117	Rapid7	IDS /IPS, Application, Authentication	UserInsight	JSON		rapid7_userinsight

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
118	RedHat	Applications	JBOSS Application Server	syslog		jboss_app_server
119	Reservoir Labs	IDS / IPS	RScope	syslog	✓	rscope_conn, rscope_dns, rscope_files, rscope_ssl, rscope_http, rscope_syslo, rscope_weird
120	Riverbed Technology	Firewall / Applications / Host / Server / Web Content / Filtering	SteelApp (formerly Web App Firewall)	syslog		riverbed
121	RSA	Host / Server / Applications / Security	RSA Authentication Manager	syslog		rsa_auth_mgr
122	RSA	Authentication	Authentication Manager	syslog		rsa_auth_mgr
123	RSyslog	Log Processor	RSyslog	syslog		rsyslog
124	Salt Stack	Application	Minion	syslog		salt_minion
125	Squid	Application	Cxtracker	syslog		unix_cxtracker
126	Shibboleth	Authentication	SSO	syslog		shibboleth_sso
127	snmpd	SNMP	snmpd	syslog		snmpd
128	Sophos	Firewall/Web & Email protection	Unified Threat Management	syslog		sophos
129	Sourcefire	IDS / IPS	Snort	syslog		sourcefire, snort
130	Splunk	Aggregator	Enterprise Forwarder	syslog		splunk
131	Squid	Web Content / Filtering / Proxies	HTTP Proxy	syslog		squid_http_proxy

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
132	stunnel	Encryption	stunnel SSL Encryption Wrapper	syslog		stunnel
133	Suricata	IPS / IDS	Suricata IDS	syslog		suricata_ips
134	Suricata	Web Content / Filtering / Proxies	Suricata Web Proxy	syslog		suricata_http_proxy
135	Symantec	Email Security	BrightMail	syslog		symantec_brightmail
136	Symantec	Antivirus / Malware	EndPoint Protection	syslog		symantec_http_proxy
137	TrendMicro	IPS / IDS	HIDS / IDS	syslog		n/a
138	TrendMicro	Antivirus / Malware	Enterprise Antivirus	syslog		n/a
139	TripWire	IDS / IPS	IDS	syslog		tripwire_ids
140	Trustwave	Web Content / Filtering / Proxies	HTTP Proxy	syslog		trustwave_http_proxy
141	Unix/OSC	Application	ABRT	syslog		unix_abrt
142	Unix/OSC	Application /Scheduling	Anacron	syslog		unix_anacron
143	Unix/OSC	Application /Scheduling	ATD	syslog		unix_atd
144	Unix/OSC	Application / OS Auditing	Audit	syslog		unix_audit
145	Unix/OSC	Application /Scheduling	Cron	syslog		unix_cron
146	Unix/OSC	Application/ Network Monitoring	CxTracker	syslog		unix_cxtracker
147	Unix/OSC	Application / OS	Init	syslog		unix_init

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
148	Unix/OSC	Application / OS	Kernel	syslog		unix_kernel
149	Unix/OSC	Application / Database	Kprop	syslog		unix_kprop
150	Unix/OSC	Application / High Availabitly - Fail Over	HA/mgmtmd	syslog		unix_mgmtmd
151	Unix/OSC	Application / Monitoring	Mon	syslog		unix_mon
152	Unix/OSC	Application / High Availabitly - Fail Over	MultiPath	syslog		unix_multipath
153	Unix/OSC	Application / Monitoring	Nagios Remote Plugin Executor	syslog		unix_nrpe
154	Unix/OSC	IDS / IPS	OSSEC	syslog		unix_ossec
155	Unix/OSC	Application / Authentication	Pluggable Authentication Module (PAM)	syslog		unix_pam
156	Unix/OSC	Application / Interface	Small Computer System Interface	syslog		unix_scsi
157	Unix/OSC	Application / Authentication / Remote Access	Secure Shell Daemon (SSHd)	syslog		unix_ssh
158	Unix/OSC	Application / Time Synchronization	Network Time Protocol Daemon	syslog		unix_xntpd
159	Varonis	Applications	DataPrivilege	syslog		varonis_dataprivilege

	Vendor	Device Type	Device Name (s)	Parser/ Method of Collection	FEYE Partner	TAP Class
160	Verdasys	Access Control	Digital Guardian	syslog		verdasys_digital_guardian
161	VMware	Virtual Hardware	ESX, ESXi	syslog		vmware_esx
162	Vormetric	Authentication / Application, File encryption	Data Security Manager, Enterprise Encyption File System	syslog		vormetric_dsm, vormetric_vfs
163	WatchGuard	Firewall	Firewall	syslog		watchguard_firewall
164	Websense	Web Content / Filtering / Proxies	HTTP Proxy	syslog		websense_http_proxy
165	ZeroFOX	Applications	ZeroFox Threat Feeds	syslog		zerofox_threat_feed