THE Simple SOLUTION

ALIENVAULT USM APPLIANCE PLUGINS LIST

This is the current plugin library that ships with AlienVault® USM Appliance™ as of **November 14, 2017.**

The AlienVault Labs Security Research Team regularly updates the plugin library to increase the extensibility of USM Appliance. These plugins enable your USM Appliance to process and analyze logs produced by your existing devices and applications quickly.

Don't see your plugin here? Ask us and we can build one for you! Submit your request here.

Plugin Name	Vendor	Model
a10-thunder-waf	A10	Thunder WAF
actiontec	Actiontec	Verizon FIOS router
netvanta	Adtran	NetVanta
aerohive-wap	Aerohive Networks	Wireless Access Point
alcatel	Alcatel	Arista Switch
allot	Allot Communications	NetEnforcer
amun-honeypot	Amun	Amun Honeypot
assp	Anti-Spam SMTP Proxy	Anti-Spam SMTP Proxy
apache-ldap	Apache Software Foundation	OpenLDAP
apache-syslog	Apache Software Foundation	Apache HTTP Server
apache-tomcat	Apache Software Foundation	Tomcat
apache	Apache Software Foundation	Apache HTTP Server
spamassassin	Apache Software Foundation	SpamAssassin
airport-extreme	Apple	AirPort Extreme
os-x	Apple	OS-X
pravail-aps	Arbor Networks	Pravail APS
arista-switch	Arista	Switches
arpalert-idm	Arpalert	Arpalert
arpalert-syslog	Arpalert	Arpalert
artemisa	Artemisa	Artemisa Honeypot
artica	Artica	Proxy
aruba-6	Aruba Networks	Wireless
aruba-airwave	Aruba Networks	Airwave
aruba-clearpass	Aruba Networks	ClearPass
aruba	Aruba Networks	Mobility Access Switches
asterisk-voip	Asterisk	VoIP
asus-router	AsusTek	Wireless Router
tarantella	Automation Access	Tarantella

avast	Avast	Free Antivirus
avaya-gateway	Avaya	Media Gateway
avaya	Avaya	VSP switches
barracuda-link-balancer	Barracuda	Link Balancer
barracuda-ng	Barracuda	Next Gen Firewall
barracuda-spam	Barracuda	Spam Firewall
barracuda-sslvpn	Barracuda	SSL VPN
barracuda-waf	Barracuda	Web Application Firewall
barracuda-webfilter	Barracuda	Web Filter
bluecoat	Blue Coat	ProxySG
bomgar	Bomgar	Remote Support and Privileged Access
bro-ids	Bro	Bro NSM
netkeeper-fw	Broadweb	IPS-Netkeeper
netkeeper-nids	Broadweb	Netkeeper NIDS
brocade	Brocade	Brocade Devices
vyatta	Brocade	Vyatta vRouter
bit9	Carbon Black	Enterprise Protection
bit9_v7	Carbon Black	Enterprise Protection
carbonblack	Carbon Black	Enterprise Response
cb-defense	Carbon Black	Defense
cerberus-ftp	Cerberus	FTP Server
checkpoint-mepp	Check Point	Media Encryption and Port Protection
fw1-alt	Check Point	FireWall
packetwave	Ciena	Packetwave
cisco-3030	Cisco	VPN 3000 Series
cisco-ace	Cisco	ACE Application Control Engine
cisco-acs-idm	Cisco	ACS Secure Access Control Server
cisco-acs	Cisco	ACS Secure Access Control Server
cisco-asa	Cisco	ASA Adaptive Security Appliance
cisco-asr	Cisco	ASR Aggregation Services Router
cisco-call	Cisco	Call Manager
cisco-esa	Cisco	AsyncOS Email Security Appliances
cisco-firepower	Cisco	FirePower NGIPS
cisco-firesight	Cisco	Firesight
cisco-fw	Cisco	Firewall Services Module
cisco-ids	Cisco	IDS Intrusion Detection System
cisco-ips-syslog	Cisco	IPS Intrusion Prevention System
cisco-ips	Cisco	IPS Intrusion Prevention System

cisco-isa	Cisco	ISA
cisco-ise	Cisco	ISE
cisco-meraki	Cisco	Meraki
cisco-nexus-nx-os	Cisco	NX-OS
cisco-ngips	Cisco	Next Generation Intrusion Prevention System NGIPS
cisco-pix	Cisco	PIX Private Internet eXchange
cisco-router	Cisco	Router
cisco-rv	Cisco	RV Series VPN Router
cisco-ucs	Cisco	Unified Computing System
cisco-vpn	Cisco	VPN
cisco-wlc	Cisco	Wireless LAN Controller
ironport	Cisco	IronPort
opendns	Cisco	OpenDNS Enterprise Insights
StealthWatch	Cisco	Lancope StealthWatch
citrix-netscaler	Citrix Systems	NetScaler
clamav	ClamAV	ClamAV
clamwin-nxlog	ClamWin	ClamWin Free Antivirus
passwordstate	ClickStudios	Passwordstate
cloudpassage	CloudPassage	Halo
comodo-antivirus	Comodo	Antivirus
corero-ips	Corero	IPS
courier	Courier-MTA	Courier Mail Server
crowdstrike	CrowdStrike	Falcon Host
cyberark	CyberArk	Enterprise Password Vault
cyberguard	CyberGuard	SG565
cylance	Cylance	CylancePROTECT
cyphort	Cyphort	Cyphort APT Defense Platform
dlink-wireless	D-Link	Unified Wireless Controller
failsafe	Damballa	FailSafe
darktrace	Darktrace	DCIP
datto-siris	Datto	Siris Platform
dell-chassis	DELL	M1000 Chassis
dell-equallogic	Dell	EqualLogic
dell-force	DELL	Force10 Switches
dell-secureworks	DELL	SecureWorks
emc-isilon	DELL	EMC Isilon
emc-vnxe	DELL	EMC VNXe

sonicwall-vpn	DELL	SonicWall VPN
sonicwall	DELL	SonicWALL Scrutinizer
dionaea	Dionaea	Dionaea Honeypot
dovecot	Dovecot	Secure IMAP Server
draytek-vigor	DrayTek	Vigor
drupal-wiki	Drupal	Drupal CMS
iprism	Edgewave	iPrism
dragon	Enterasys	Dragon IDS
enterasys-rmatrix	Enterasys	Matrix N-Series
airlock	Envault	Airlock
eset	Eset	Eset
redtrust	Evolium	Redtrust
silvershield	Extenua	SilverSHielD
extreme-switch	Extreme Networks	Switch
extreme-wireless	Extreme Networks	Summit Series
f5-firepass	F5	FirePass SSL VPN
f5	F5	BIG-IP
fail2ban	Fail2ban	Fail2ban
falconstor	FalconStor Software	IPStor
fireeye-cm	FireEye	CM
fireeye-hx	FireEye	HX Series
fireeye	FireEye	MPS
triton	ForcePoint	Triton AP-Web
forescout-nac	ForeScout	CounterACT
fortiWLC	Fortinet	fortiWLC
fortiauthenticator	Fortinet	FortiAuthenticator
fortigate	Fortinet	FortiGate
fortiguard	Fortinet	FortiGuard
fortimail	Fortinet	FortiMail
fortiweb	Fortinet	Fortiweb
meru	Fortinet	Meru Networks WLAN Controller
ipfw	FreeBSD	IPFW Firewall
ntpdate	FreeBSD	NTPdate
freeipa	FreeIPA	FreeIPA
freeradius	FreeRADIUS	freeradius
axigen-mail	GeCAD	Axigen Mail Server
gfi	GFI	Vipre Antivirus
gta-firewall	Global Technology Associates	Firewall

h3c-ap	H3C	AP
h3c-switch	H3C	Ethernet Switch
ha-proxy	HAProxy	HAProxy
harpp-ddos	HARPP	HARPP DDoS Mitigator
hitachi-hnas	Hitachi	NAS Platform
honeyd	Honeyd	Honeyd Virtual Honeypot
glastopng	Honeynet Project	GlastopfNG Honeypot
nepenthes	Honeynet Project	Nepenthes Honeypot
hp-chassis	HP	BladeSystem Chassis
hp-eva	HP	EVA Storage
hp-san-switch	HP	SAN Switch
hp-switch	HP	Switch
hp-wireless	HP	E-Series Mobility
serviceguard	HP	Serviceguard
sitescope	HP	SiteScope
huawei-ips	Huawei	IPS
huawei-router	Huawei	Enterprise Router
huawei	Huawei	NG-Firewall
aix-audit	IBM	Aix Audit
as400	IBM	AS400
fidelis	IBM	Fidelis Network Data Loss Protection
ibm-imm	IBM	Integrated Management Module
ibm-tam	IBM	Tivoli Access Manager WebSEAL
ibm-websphere	IBM	Websphere
raslogd	IBM	RASlog
realsecure	IBM	RealSecure Server Sensor
siteprotector-snmp	IBM	Proventia IPS
storewize-V7000	IBM	Storwize V7000
vplus	IBM	VisionPLUS
siteprotector-iss	IBM Internet Security Systems	Site Protector
siteprotector	IBM Internet Security Systems	Site Protector
eljefe	Immunity	El Jefe
imperva-securesphere	Imperva	SecureSphere
incapsula	Imperva	Incapsula WAF
impravata-onesign	Imprivata	Onesign
infoblox	Infoblox	DNS Server
snare-idm	Intersect Alliance	Snare

snare-mssql	Intersect Alliance	Snare
snare-msssis	Intersect Alliance	Snare
snare	Intersect Alliance	Snare
bind	ISC	BIND
juniper-ex	Juniper Networks	EX Series
juniper-idp	Juniper Networks	IDP Series
juniper-mx	Juniper Networks	MX Routers
juniper-nsm	Juniper Networks	NSM Network and Security Manager
juniper-srx	Juniper Networks	SRX Series
juniper-vpn	Juniper Networks	SA Secure Access Series
netscreen-firewall	Juniper Networks	NetScreen Series Firewall
netscreen-igs	Juniper Networks	ISG Series
netscreen-manager	Juniper Networks	NetScreen Security Manager
netscreen-nsm	Juniper Networks	NetWork and Security Manager
kaspersky-sc	Kaspersky	Security Center
kaspersky	Kaspersky	Antivirus
kemp	Kemp Technologies	VLM-2000-W
kismet	Kismet	Kismet Wireless
linuxdhcp-idm	Linux	DHCP Server
linuxdhcp	Linux	DHCP
nfs	Linux	NFS Network File System
heartbeat	Linux-HA	Heartbeat
logbinder-sp	LOGbinder	LOGbinder for SharePoint
lucent-brick	Lucent	VPN Firewall Brick
m0n0wall	M0n0wall	M0n0wall Embedded Firewall
malwarebytes-br	Malwarebytes	Breach Remediation
malwarebytes-es	Malwarebytes	Endpoint Security
malwarebytes	Malwarebytes	Malwarebytes
password-manager-pro	Manage Engine	Password Manager Pro
adaudit-plus	ManageEngine	ADAudit Plus
intrushield	McAfee	IntruShield IPS
mcafee-antispam	McAfee	Anti-Spam
mcafee-db	McAfee	Database Security
mcafee-epo	McAfee	ePolicy Orchestrator
mcafee-mwg	McAfee	McAfee-MWG
mcafee	McAfee	Network Security Platform
mcafee	McAfee	Antivirus Engine
sidewinder	McAfee	Firewall Enterprise

dhcp-nxlog	Microsoft	DHCP Client Service
dhcp	Microsoft	DHCP Client Service
emet	Microsoft	Enhanced Mitigation Experience Toolkit
exchange-nxlog	Microsoft	Exchange Server
exchange	Microsoft	Exchange Server
iis-nxlog	Microsoft	IIS Internet Information Services
iis	Microsoft	IIS Internet Information Services
isa	Microsoft	ISA Internet Security and Acceleration Server
microsoft-ata	Microsoft	Advanced Threat Analytics
ms-sccm	Microsoft	System Center Configuration Manager
mssql-audit	Microsoft	MSSQL
mssql-nxlog	Microsoft	SQL Server
multifactor-auth	Microsoft	Multi-Factor Authentication
nxlog	Microsoft	Windows
o365-asm	Microsoft	Office 365 Advanced Security Management
windns-nxlog	Microsoft	DNS Server
windns	Microsoft	DNS Server
mikrotik-router	MikroTik	Router
moodle	Moodle	Moodle
motorola-firewall	Motorola	RFS Series
mwcollect	Mwcollect	Mwcollect Honeypot
netasq-u	Netasq	U-Series
netgear-switch	NETGEAR	Switch
netgear	Netgear	FVS318 ProSafe VPN Firewall
nginx	NGinX	NGinX
nimble-storage	Nimble	Nimble-OS
alteonos	Nortel Networks	Alteon
nortel-baystack	Nortel Networks	Baystack Ethernet Switch
nortel-switch	Nortel Networks	Passport 1612 Switch
ntsyslog	NTSyslog	NTSyslog
suricata-eve	OISF	Suricata
powerdns	Open-Xchange	PowerDNS
pf	OpenBSD	PF Packet Filter
ssh-remote	OpenBSD	OpenSSH
ssh	OpenBSD	OpenSSH
openldap	OpenLDAP	OpenLDAP
opennms-monitor	OpenNMS	OpenNMS

openswan	OpenSwan	IPsec
optenet	Optenet	MailSecure
oracle-syslog	Oracle	Database Server
palerra	Oracle	Palerra Cloud Security
radiator	OSC	Radiator RADIUS Server
osiris	Osiris	Osiris HIDS
osquery	OSquery	OSquery
owncloud	OwnCloud	OwnCloud
packetfence	PacketFence	PacketFence
paloalto	Palo Alto Networks	PA-5000 Series
panda-as	Panda Security	AdminSecure
panda-se	Panda Security	Security for Enterprise
postfix	Postfix	Postfix
postgresql	PostgreSQL GDG	postgresql
prads	Prads	Prads
proftpd	ProFTPD	ProFTPD
proofpoint-ps	Proofpoint	Protection Server
proofpoint-tap	Proofpoint	Targeted Attack Protection
proxim-orinoco	Proxim	Orinoco AP700
pureftpd	Pure-FTPd	Pure-FTPd
qnap-qts	QNAP	QTS
defender-tokengo	Quest Software	Defender GO-6 Token
quickheal-blockedapp	Quick Heal	SQEPS6.3
quickheal-fileact	Quick Heal	SQEPS6.3
quickheal-firewall	Quick Heal	SQEPS6.3
quickheal-vulscan	Quick Heal	SQEPS6.3
radware-ips	Radware	DefensePro
clurgmgr	Red Hat	Resource Group (Cluster Service) Manager Daemon
jboss	Red Hat	JBoss Middleware
redhat-audit	Red Hat	Audit
rrd	RRDtool	RRDtool
rsa-authentication-manager	RSA	Authentication Manager
rsa-secureid	RSA	SecurID
token-rsa	RSA	SecurID Software Token Converter
rsa-securid-idr	RSA Security	SecurID IDR
ruckus	Ruckus	ZoneDirector
aladdin	SafeNet	eSafe

smbd	Samba	Samba SMB
samhain	Samhain Labs	Samhain
sangfor	Sangfor	NGFW
sap	SAP	NetWeaver
secureauth	SecureAuth	SecureAuth
sendmail	SendMail	SendMail
shorewall	Shorewall	Shorewall
shrubbery-tacacs	Shrubbery Networks	TACACS+
tacacs-plus	Shrubbery Networks	TACACS+
siteminder	SiteMinder	Policy-Server
snort_syslog	Snort	Snort
cyberoam	Sophos	Cyberoam-Firewall
sophos-central	Sophos	Central
sophos-ec	Sophos	EC
sophos-es	Sophos	ES
sophos-mssql	Sophos	Antivirus
sophos-utm	Sophos	Sophos-UTM
sophos-ws	Sophos	Secure Web Gateway
sophos	Sophos	XG
sophos	Sophos	Antivirus
sourcefire-ids	Sourcefire	Defense Center
squid	Squid	Squid Cache Proxy
squidGuard	SquidGuard	SquidGuard
stonegate	Stonesoft	StoneGate
stonegate_ips	Stonesoft	IPS
stormshield	Stormshield	Netasq NG
sudo	Sudo	Sudo
suhosin	Suhosin	Suhosin PHP Security Extension
iptables	Suse	IPTables
symantec-ams	Symantec	AMS
symantec-atp	Symantec	ATP
symantec-epm	Symantec	Endpoint Protection
symantec-mg	Symantec	Messaging Gateway
synology	Synology	DiskStation
syslog	Syslog	Syslog
tanium	Tanium	EndPoint Platform
nessus-detector	Tenable	Nessus
nessus	Tenable	Nessus

tesserent-ng	Tesserent	Managed Next Gen Firewall
spamtitan	TitanHQ	SpamTitan
deepsec-agent	Trend Micro	Deep Security Agent
deepsec-manager	Trend Micro	Deep Security Manager
tippingpoint	Trend Micro	TippingPoint IPS
trendmicro-cm	Trend Micro	Control Manager
trendmicro	Trend Micro	InterScan Messaging Security
trustwave	Trustwave	Secure Web Gateway
modsecurity	TrustWave SpiderLabs	ModSecurity Web Application Firewall
tufin	Tufin	Tufin Orchestration Suite
ubiquiti-unifi	Ubiquiti	Unifi
pam_unix	UNIX	PAM Pluggable Authentication Module
untangle-ngfw	Untangle	NG Firewall
vandyke-vshell	VanDyke	VShell
vectra	Vectra	X-Series
vmware-esxi	VMware	ESXi
vmware-vcenter-sql	VMware	vCenter
vmware-vcenter	VMware	vCenter
vmware-view-admin	VMWare	View Administrator
vmware-vshield	VMware	vShield
vmware-workstation	VMware	WorkStation
vormetric-dsm	Vormetric	Data Security Manager
vsftpd	Vsftpd	Vsftpd
watchguard	WatchGuard	XTM Series
webmin	Webmin	Webmin
webroot-flowscape	Webroot	FlowScape
websense-content	Websense	Content Gateway
websense-esg	Websense	Email Security Gateway
websense	Websense	Web Security Gateway
websense7	Websense	Web Security Gateway
wing-ftp-server	Wing FTP Software	Wing FTP Server
wuftp	WU-Ftp	WU_Ftp
ascenlink	Xtera	AscenLink
yara	Yara	Yara
zerofox	ZeroFox	Social Media Security SAAS Platform
zscaler	zScaler	Nanolog
zyxel-firewall	ZyXEL	ZyWALL