ALIENVAULT® USM ANYWHERE™ PLUGINS LIST

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

The AlienVault Labs Security Research Team regularly updates the plugin library to increase the extensibility of USM Anywhere. These plugins enable your USM Anywhere 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	Device	DeviceType
AWS Application Load Balancer	Amazon	Application Load Balancer	Load Balancer
ServerAccess	Amazon	aws	Cloud Infrastructure
ELBAccess	Amazon	Classic Load Balancer	Load Balancer
CloudFront RTMP distribution W3C	Amazon	CloudFront	Proxy
CloudFront Web distribution W3C	Amazon	CloudFront	Proxy
Amazon AWS CloudTrail	Amazon	CloudTrail	Cloud Infrastructure
Amazon Macie	Amazon	Macie	Cloud Infrastructure
Route 53 DNS Queries	Amazon	Route 53	DNS Server
VPC Flow Logs	Amazon	VPC	Cloud Infrastructure
Apache	Apache	apache	Web Server
Apple Airport Extreme	Apple	Airport Extreme	Router/Switch
Arbor Networks Pravail APS	Arbor Networks	Pravail APS	Load Balancer
Aruba Clearpass	Aruba Networks	Clearpass	Network Access Control
Aruba ClearPass CEF	Aruba Networks	ClearPass	Network Access Control
Aruba	Aruba Networks	Wireless	Wireless Security/Management
Asterisk VoIP	Asterisk	VoIP	Server
Avaya Media Gateway	Avaya	Media Gateway	Server
Avaya Wireless LAN	Avaya	Wireless LAN	Wireless Security/Management
Avaya VSP Switches	Avaya Networks	VSP Switches	Router/Switch
Barracuda Web Application Firewall	Barracuda	Firewall	Application Firewall
Barracuda NextGen Firewall	Barracuda	NextGen Firewall	Firewall
Barracuda NextGen Firewall Traffic	Barracuda	NextGen Firewall	Firewall
Barracuda Spam Firewall	Barracuda	Spam Firewall	Mail Security
Barracuda Web Application Firewall CEF	Barracuda	WAF	Application Firewall
Barracuda Web Filter	Barracuda	Web Filter	Proxy
Bluecoat W3C	Blue Coat	BlueCoat	Proxy
Box Events	Box	Box	Cloud Application
Brocade	Brocade	Brocade	Router/Switch
cb Defense	Carbon Black	Cloud Antivirus System	Antivirus

cb Response	Carbon Black	Endpoint Security	Endpoint Security
cb Protection	Carbon Black	Security Platform	Endpoint Security
CheckPoint FW1	Check Point	FW1	Firewall
CheckPoint FW1 Loggrabber	Check Point	FW1 Loggrabber	Firewall
CheckPoint FW1 Generic	Check Point	generic	Firewall
CheckPoint FW1 R77.3O	Check Point	R77.30	Firewall
Cisco ACE	Cisco	ACE	Router/Switch
Cisco ACS	Cisco	ACS	Unified Threat Management
Cisco ASA	Cisco	ASA	Firewall
Cisco ASR	Cisco	ASR	Router/Switch
Cisco Umbrella	Cisco	Cisco Umbrella	Network Access Control
Cisco Firesight	Cisco	Firesight	Unified Threat Management
SourceFire IDS	Cisco	IDS	Intrusion Detection
Cisco Ironport	Cisco	Ironport	Mail Security
Cisco Lancope StealthWatch	Cisco	Lancope StealthWatch	Intrusion Detection
Cisco Meraki	Cisco	Meraki	Wireless Security/Management
Cisco Nexus	Cisco	Nexus	Router/Switch
Cisco Firepower NGIPS	Cisco	NGIPS	Intrusion Prevention
Cisco Pix	Cisco	Pix	Firewall
Cisco Router	Cisco	Router	Router
Snort Syslog	Cisco	snort	Intrusion Detection
Cisco VPN	Cisco	VPN	VPN
Cisco WLC	Cisco	WLC	Wireless Security/Management
Citrix Netscaler Application Firewall CEF plugin	Citrix	Citrix Netscaler	Application Firewall
Citrix NetScaler	Citrix	NetScaler	Load Balancer
Cloudflare Enterprise Log Share	Cloudflare	Enterprise Log Share	Cloud Infrastructure
CloudPassage CEF	CloudPassage	CloudPassage	Unified Threat Management
Endpoint Protector	CoSoSys	Endpoint Protector	Data Loss Prevention
CrowdStrike Falcon	CrowdStrike	Falcon Host	Endpoint Protection
CyberArk Enterprise Password Vault	CyberArk	Enterprise Password Vault	Data Protection
Cylance CylancePROTECT	Cylance	CylancePROTECT	Endpoint Security
Cyphort CEF plugin	Cyphort	Cyphort	Unified Threat Management
D-Link UTM Firewall	D-Link	D-Link UTM Firewall	Firewall
Darktrace Cyber Intelligence Platform	Darktrace	DCIP	Anomaly Detection
Dell SecureWorks	Dell	SecureWorks	Unified Threat Management
Dell SonicWall UTM	Dell	SonicWall UTM	Unified Threat Management
Docker	Docker	Daemon	Container Infrastructure

Eset	Eset	Eset	Antivirus
F5 Big-ip	F5	Big-ip	Load Balancer
Fail2ban	Fail2ban	Fail2ban	Intrusion Prevention
FireEye Central Management System	FireEye	CMS	Unified Threat Management
FireEye Endpoint Security HX Series	FireEye	HX	Endpoint Security
FireEye Malware Protection Systems	FireEye	MPS	Unified Threat Management
Forcepoint Triton AP-Web	Forcepoint	Triton AP-Web	Proxy
ForeScout NAC	ForeScout	NAC	Network Access Control
Fortinet Fortigate	Fortinet	Fortigate	Firewall
FreeRadius	FreeRADIUS	FreeRadius	Network Access Control
G Suite Audit	Google	Google Apps	Application
G Suite Drive	Google	Google Apps	Application
H3C Switch	H3C	Switch	Switch
HAProxy	HAProxy	haproxy	Load Balancer
HP Storage Area Network Switch	HP	SAN Switch	Switch
HP Switch	HP	Switch	Switch
Huawei NGFW	Huawei	Next-Generation Firewall	Firewall
AIX Audit	IBM	Audit	Operating System
IBM Tivoli Access Manager WebSEAL	IBM	Tivoli Access Manager WebSEAL	Proxy
Imperva SecureSphere	Imperva	SecureSphere	Application Firewall
Imperva SecureSphere CEF	Imperva	SecureSphere	Application Firewall
Incapsula CEF plugin	Incapsula	Incapsula	Application Firewall
Linux BIND	ISC	BIND	DNS Server
JumpCloudAPI	JumpCloud	JumpCloudAPI	Cloud Infrastructure
Juniper EX Series	Juniper	EX Series	Router/Switch
Juniper Network Security Manager	Juniper	Juniper Network Security Manager	Unified Threat Management
Juniper NetScreen ScreenOS	Juniper	NetScreen ScreenOS	Firewall
Juniper NetScreen ScreenOS Traffic	Juniper	NetScreen ScreenOS	Firewall
Juniper Secure Access VPN	Juniper	Secure Access VPN	VPN
Juniper SRX Junos	Juniper	SRX Junos	Unified Threat Management
Kaspersky Security Center	Kaspersky	Security Center	Antivirus
Kaspersky Security Center CEF	Kaspersky	Security Center	Antivirus
Linux ClamAV	Linux	ClamAV	Antivirus
Linux DHCP client	Linux	dhclient	Authentication and DHCP
Linux DHCPD	Linux	DHCPD	Authentication and DHCP
Linux IPTables	Linux	IPTables	Firewall
Linux Auditd	Linux	Linux	Operating System
Linux CRON	Linux	Linux	Application
Linux SUDO	Linux	Linux	Authentication and DHCP

UFW	Linux	UFW	Firewall
Malwarebytes Breach Remediation	Malwarebytes	Breach Remediation	Antivirus
Malwarebytes Endpoint Security	Malwarebytes	Endpoint Security	Endpoint Security
Malwarebytes Management Console	Malwarebytes	Management Console	Antivirus
McAfee Database Security	McAfee	Database Security	Infrastructure Monitoring
McAfee EPO	McAfee	McAfee EPO	Antivirus
McAfee Network Security Platform	McAfee	Network Security Platform	Intrusion Prevention
McAfee Web Gateway	McAfee	Web Gateway	Proxy
Microsoft Advanced Threat Analytics	Microsoft	Advanced Threat Analytics	Unified Threat Management
AWSWindows	Microsoft	AWS-Windows	Operating System
Microsoft IIS 8.0+ Plugin	Microsoft	AWS-Windows-IIS	Web Server
Microsoft IIS pre-8.0 Plugin	Microsoft	AWS-Windows-IIS	Web Server
Office 365 Azure AD	Microsoft	Azure AD	Authentication
Azure Insight	Microsoft	Azure Cloud	Cloud Infrastructure
Azure IIS	Microsoft	Azure IIS	Web Server
Azure Security Center	Microsoft	Azure Security Center	Cloud Infrastructure
Azure SQL Server	Microsoft	Azure SQL Server	Database
Azure Web App	Microsoft	Azure Web App	Web Server
Azure Windows Events	Microsoft	Azure Windows	Operating System
Office 365 Exchange	Microsoft	Exchange	Mail Server
Windows IIS NxLog	Microsoft	IIS NxLog	Web Server
Office 365 Audit	Microsoft	Office 365 Audit	Cloud Infrastructure
Office 365 SharePoint	Microsoft	SharePoint	Cloud Application
Windows Snare	Microsoft	snare	Operating System
Windows NxLog	Microsoft	Windows NxLog	Operating System
Windows Winlogbeat	Microsoft	WinLogBeat	Operating System
MikroTik Router	MikroTik	MikroTik Router	Router/Switch
Nginx	NGinX	nginx	Web Server
Nimble Storage	Nimble	Nimble-OS	Data Protection
Okta	Okta	Okta	Authentication
PowerDNS	Open-XChange	PowerDNS	DNS Server
Linux SSH	OpenSSH	Linux	Authentication and DHCP
Oracle Audit Syslog	Oracle	Oracle	Database
Osquery	Osquery	Osquery	Endpoint Security
PacketFence	PacketFence	PacketFence	Network Access Control
Paloalto PAN-OS	PaloAlto	PaloAlto PAN-OS	Firewall
Percona Audit Log	Percona	Percona Audit Log	Infraestructure Monitoring
pfSense Filter	pfSense	pfSense	Firewall
Postfix	Postfix	postfix	Mail Server
ProFTPD	ProFTPD	ProFTPD	Server

Riverbed STM	Riverbed	Riverbed Stingray Traffic Manager	Application Delivery Controller
RSA Authentication Manager	RSA	Authentication Manager	Authentication and DHCP
Ruckus Wireless ZoneDirector	Ruckus	Wireless	Wireless Security/Management
Salesforce Activity	Salesforce	SalesForce	Cloud Infrastructure
Sangfor Next-Generation Firewall	Sangfor	NGFW	Firewall
SendMail	Sendmail	SendMail	Mail Server
SentinelOne	SentinelOne	SentinelOne	Endpoint Security
Shrubbery Tacacs	Shrubbery Networks	Tacacs	Authentication and DHCP
Sophos Cyberoam	Sophos	Cyberoam	Firewall
Sophos Enterprise Console	Sophos	Enterprise Console	Antivirus
Sophos Central	Sophos	Sophos Central	Unified Threat Management
Sophos UTM	Sophos	Sophos UTM	Unified Threat Management
Sophos Web Security	Sophos	Web Security	Proxy
Sophos XG	Sophos	XG	Firewall
SpyCloud	SpyCloud	SpyCloud	Data Protection
Squid	Squid	Squid	Proxy
Symantec ATP	Symantec	Advanced Threat Protection	Endpoint Security
Symantec DLP	Symantec	Advanced Threat Protection	Endpoint Security
Symantec EPM	Symantec	EPM	Endpoint Security
Syncplify.me	Syncplify	Syncplify.me Server!	FTP Server
Tesserent Next Gen Firewall	Tesserent	Next Gen Firewall	Firewall
Trend Micro Control Manager	Trend Micro	Control Manager	Endpoint Security
Trend Micro Deep Security	Trend Micro	Deep Security	Endpoint Security
OSSEC JSON	Trend Micro	OSSEC	Endpoint Security
OSSEC v2.5	Trend Micro	Ossec	Endpoint Security
Trustwave Secure Web Gateway	Trustwave	Secure Web Gateway	Proxy
Trustwave Secure Web Gateway Traffic	Trustwave	Secure Web Gateway	Proxy
Vectra	Vectra	Vectra	Intrusion Detection
VMware Esxi	VMware	Esxi	Other Devices
VMware vCenter	VMware	vCenter	Management Platform
VMware SSO	VMware	vCenter Single-Sign-On	Network Access Control
VMwareAPI	VMware	VMwareAPI	Infrastructure Monitoring
VMware vShield	VMware	vShield	Management Platform
Watchguard XTM	Watchguard	XTM	Unified Threat Management
Wazuh	Wazuh	Wazuh OSSEC	Endpoint Security
Webroot FlowScape	Webroot	FlowScape	Anomaly Detection
Websense Email Security Gateway	Websense	Email Security Gateway	Mail Security
Websense Web Security Gateway	Websense	Web Security Gateway	Application Firewall

Windows DNS Server	Windows	DNS Server	DNS Server
ZeroFOX	ZeroFOX	ZeroFOX	Other Devices
zScaler NSS	zScaler	Nanolog Streaming Service	Proxy
ZyXEL ZyWALL	ZyXEL	ZyWALL	Firewall