



Integration Guide

AlienVault Unified Security Management™ (USM)

About This Guide

Guide Type

Documented Integration — WatchGuard or a Technology Partner has provided documentation demonstrating integration

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

AlienVault USM Integration Overview

This document describes how to configure a WatchGuard Firebox to send log data to AlienVault USM.

Platform and Software

The hardware and software used to complete the steps outlined in this document include:

- Firebox or WatchGuard XTM device installed with Fireware v11.10.x
- AlienVault-USM_trial_5.2.2 with a Virtual Appliance

Configuration

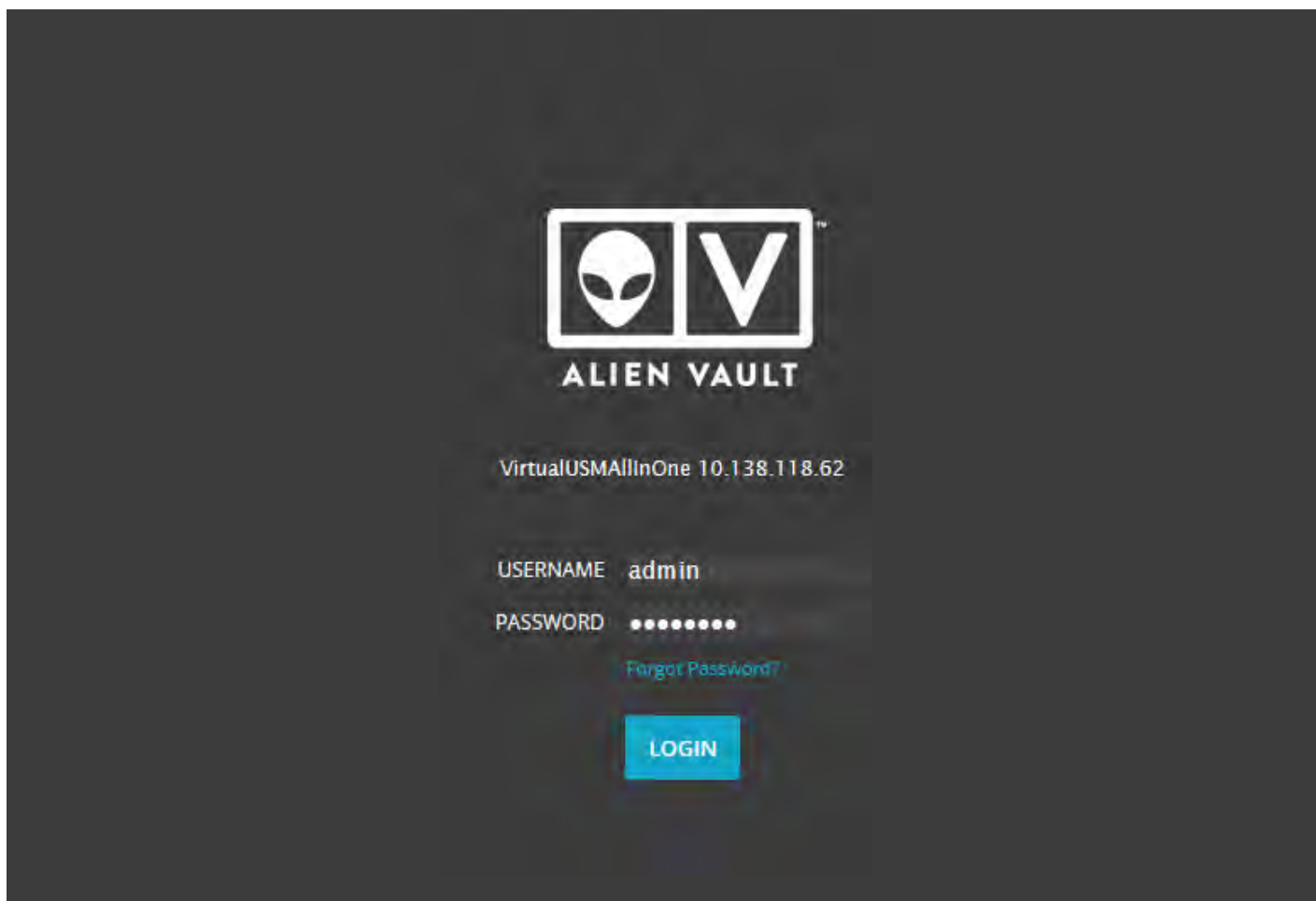
To complete this integration, you must first deploy AlienVault USM. In our integration tests, we used the AlienVault USM with a Virtual Appliance.



To set up the AlienVault environment, please refer to the AlienVault [Initial Setup Guide](#). In this document, we describe how to enable the WatchGuard Plugin on AlienVault USM and how it works with the WatchGuard Firebox. The WatchGuard Plugin is used with the AlienVault USM Sensor to extract and normalize syslog data received from a WatchGuard Firebox. For more information on how to enable the plugin see the AlienVault [Plugins Management Guide](#).

Set Up AlienVault USM

After AlienVault USM is deployed with a virtual appliance and you have completed the initial setup steps, launch a web browser and connect through its web UI at **https://<Management IP>**.



Add Assets

There are several ways to add an asset or assets on AlienVault USM. In this documentation, we show you how to add an asset manually. To learn more about adding assets, see the [AlienVault documentation](#).

1. Navigate to **Environment > Assets & Groups > Assets**.
2. Click **Add Assets**, and then **Add Host**. The New Asset window displays.
3. In the **Name** text box, type a name to identify the asset. In our example, we name the asset *Firebox*.
4. In the **IP Address** text box type the IP address of the Firebox. In our example, we type *10.0.1.1*.

EDIT ASSET

GENERAL PROPERTIES SOFTWARE

Values marked with (*) are mandatory

Name *
Firebox

IP Address *
10.0.1.1

FQDN/Aliases

Asset Value *
2

External Asset *
 Yes No


Sensors *
 10.138.118.62 (VirtualUSMAllInOne)

Operating System

Description

Icon Allowed format: Up to 400x400 PNG, JPG or GIF image
 Choose icon ...

Location
Undetermined location




Latitude/Longitude

Model

Devices Types
-- Devices -- Types ADD

5. The other fields are optional. Click **Save** to save the configuration.

Enable Plugin

1. Navigate to **Environment > Assets & Groups > Assets**.
2. Select the Firebox asset you just added to your AlienVault configuration.
3. Click .
4. Click the **Plugins** tab.
5. Click **Edit Plugins**.

EDIT PLUGINS

VENDOR	MODEL	VERSION
WatchGuard	XTM Series	-

ADD PLUGIN

CANCEL SAVE

- Use the drop-down menus to set the **Vendor** as *WatchGuard* and the **Model** to *XTM Series*. The **Version** is optional.

VULNERABILITIES ALARMS EVENTS SOFTWARE SERVICES **PLUGINS** PROPERTIES NETFLOW GROUPS

EDIT PLUGINS

VENDOR	MODEL	VERSION	SENSOR	RECEIVING DATA
WatchGuard	XTM Series	-	VirtualUSMAInOne [10.138.118.62]	Yes

- Click **Save**.

Set Up Your Firebox to Send Syslog Messages to AlienVault

- Connect to your Firebox with Policy Manager or Fireware Web UI. In this document, we use Policy Manager.
- Select **Setup > Logging**.

Use these settings to configure where the device sends log messages.

This device can send log messages to more than one destination at the same time. Select one or more check boxes to specify where log messages are sent: WatchGuard Log Server, syslog server, or Firebox internal storage.

WatchGuard Log Server

Send log messages to these WatchGuard Log Servers:

Log Servers 1 | Log Servers 2

The servers you specify on the **Log Servers 2** tab are only available for devices with Fireware XTM OS v11.10 and higher.

Syslog Server

Send log messages to this syslog server:

IP address: 10.0.1.2

Port: 514

Log format: Syslog

Firebox Internal Storage

Send log messages to Firebox internal storage

Send log messages when the configuration for this device is changed

OK Cancel Help

3. Enable the **Send log messages to this syslog server** check box.
4. In the **IP address** text box, type the AlienVault Management IP address. In our example, that IP address is *10.0.1.2*.
5. From the Port drop-down list, select **514**.
6. From the **Log format** drop-down list, select **Syslog**.
7. Save the configuration changes to your Firebox.

Test the Integration

Use these steps to make sure that Firebox syslog messages are correctly sent to AlienVault USM.

1. In the AlienVault web UI, navigate to **ANALYSIS > SECURITY EVENTS (SIEM)**. From the **DATA SOURCES** drop-down list, select **Watchguard** and click **GO** to search for events that were generated through the WatchGuard plugin. The Events display will look something like this:

The screenshot shows the 'SECURITY EVENTS (SIEM)' interface. At the top, there are tabs for 'SIEM', 'REAL-TIME', and 'EXTERNAL DATABASES'. A search bar contains 'Signature' and a 'GO' button. On the left, 'SHOW EVENTS' options include 'Last Day' (selected), 'Last Week', 'Last Month', and 'Date Range'. The 'DATA SOURCES' dropdown is highlighted with a green circle and set to 'Watchguard'. Other filters include 'ASSET GROUPS', 'NETWORK GROUPS', 'RISK', 'OTX IP REPUTATION', 'OTX PULSE', and 'ONLY OTX PULSE ACTIVITY'. A 'CLEAR FILTERS' button is visible. Below the filters, there are 'EVENTS', 'GROUPED', and 'TIMELINE' tabs. A 'SHOW TREND GRAPH' toggle is set to 'OFF'. The main display area shows 'DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS' and '269,509 TOTAL EVENTS IN DATABASE'. The table below has columns: SIGNATURE, DATE GMT-5:00, SENSOR, OTX, SOURCE, DESTINATION, and RISK. The first row is 'Watchguard: Denied packet' with a date of 2016-03-10 07:35:02, sensor 'VirtualUSMailInOne', source '10.138.117.26:138', and destination '10.138.117.255:138'.

SIGNATURE	DATE GMT-5:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
Watchguard: Denied packet	2016-03-10 07:35:02	VirtualUSMailInOne	N/A	10.138.117.26:138	10.138.117.255:138	0
Watchguard: Allowed packet	2016-03-10 07:34:28	VirtualUSMailInOne	N/A	172.16.1.11:60750	116.214.12.74:80	0
Watchguard: Allowed packet	2016-03-10 07:34:28	VirtualUSMailInOne	N/A	172.16.1.11:59544	116.214.12.74:443	0
Watchguard: Allowed packet	2016-03-10 07:34:25	VirtualUSMailInOne	N/A	172.16.1.11:59542	116.214.12.74:443	0
Watchguard: Allowed packet	2016-03-10 07:34:25	VirtualUSMailInOne	N/A	172.16.1.11:60748	116.214.12.74:80	0
Watchguard: Allowed packet	2016-03-10 07:34:23	VirtualUSMailInOne	N/A	172.16.1.11:59540	116.214.12.74:443	0
Watchguard: Allowed packet	2016-03-10 07:34:23	VirtualUSMailInOne	N/A	172.16.1.11:60746	116.214.12.74:80	0

2. Double-click an Event to view details.

SECURITY EVENTS (SIEM)

SIEM REAL-TIME EXTERNAL DATABASES

Security Events > Watchguard: Allowed packet < PREVIOUS NEXT >

Watchguard: Allowed packet **ACTIONS**

DATE	2016-03-10 07:34:28 GMT-5:00	CATEGORY	Access
ALIENVAULT SENSOR	VirtualUSMailinOne [10.138.118.62]	SUB-CATEGORY	Firewall Permit
DEVICE IP	10.138.118.62 [amv]	DATA SOURCE NAME	watchguard
EVENT TYPE ID	1	DATA SOURCE ID	1691
UNIQUE EVENT ID#	e69211e5-912e-000c-292e-fb30d7b0f76	PRODUCT TYPE	Unified threat management
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
2	2	0	0

SOURCE 172.16.1.11

Hostname: N/A	Location: N/A
MAC Address: N/A	Context: N/A
Port: 59544	Asset Groups: N/A
Latest update: N/A	Networks: N/A
Username & Domain: N/A	Logged Users: N/A
Asset Value: 2	OTX IP Reputation: No

SERVICE PORT PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST

DESTINATION 116.214.12.74

Hostname: N/A	Location: Taiwan
MAC Address: N/A	Context: N/A
Port: 443	Asset Groups: N/A
Latest update: N/A	Networks: N/A
Username & Domain: N/A	Logged Users: N/A
Asset Value: 2	OTX IP Reputation: No

SERVICE PORT PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST

USERDATA1	USERDATA2	USERDATA3
3-Optional-2	1-External1	3000-0148

RAW LOG

```
Msg 10 07:34:28 WatchGuard-XTM firewall: msg_id="3000-0148" Allow 3-Optional-2 1-External1 60 tcp 20 63 172.16.1.11 116.214.12.74 59544 443 offset 10 8 948722553 win 2105 (HTTPS-00)
```