



AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

Data Source Plugin Management



CONTENTS

1. INTRODUCTION.....	4
2. CONFIGURE EXTERNAL APPLICATION OR DEVICE	4
3. ENABLING DATA SOURCE PLUGINS	4
3.1. Enabling Data Source Plugins in the Asset Details Screen	5
3.2. Enabling Data source plugins In AlienVault Center	6
3.3. Enabling Data source plugins through the command line console	8
4. CONFIRM ALIENVAULT USM IS RECEIVING AND PRODUCING EVENTS	9
APPENDIX A - CONFIGURING ALIENVAULT TO RECEIVE LOGS THROUGH SYSLOG.....	11
APPENDIX B - CONFIGURING LOG FILE EXPIRATION	12
APPENDIX C - DEBUGGING CONNECTION FROM DEVICE TO ALIENVAULT	13
APPENDIX D - LIST OF INSTRUCTIONS FOR DATA SOURCE PLUGINS	14



1. INTRODUCTION

A data source plugin is a software component that provides specific support for AlienVault USM to process and analyze logs produced by external applications and devices. Data Source Plugins provides logic specific to an external application that is used by AlienVault USM to extract data from a log and enrich it with security-specific meta-data to produce an 'Event' which is managed by the AlienVault system.

Configuring a data source plugin requires the following basic steps

1. Configure external application or device to forward logs to a sensor via Syslog (or through another supported method)
2. Enabling the specific data source plugin matching the external application or device on that same sensor
3. Confirm event logs are being received and are processed

AlienVault provides a large number of data source plugins as part of your default installation (see [APPENDIX D -](#) for complete listing), in most environments this should cover the external applications and devices that you wish to integrate into AlienVault USM. It is also possible to create custom data source plugins for devices that are not supported out of the box. To learn how to create custom data source plugins refer to document “***How to create a Data Source Plugin***” for reference.

2. CONFIGURE EXTERNAL APPLICATION OR DEVICE

In order to process logs from external applications first you must configure the external application or device to forward the log to an AlienVault Component (either a dedicated Sensor or an All-in-One). The most common method to accomplish this is to use Syslog, this is supported by the large majority of vendors on the market. Configuration of Syslog will vary between products specific documentation for configuring the external applications or devices that correspond to supported data source plugins is referenced in [APPENDIX D -](#).

Detect Data Source Plugins receive log information and extract events from them. They process text log information from log files created by RSyslog collection system; and from log data retrieved from remote systems via one of the remote collection protocols such as SDEE and SFTP.

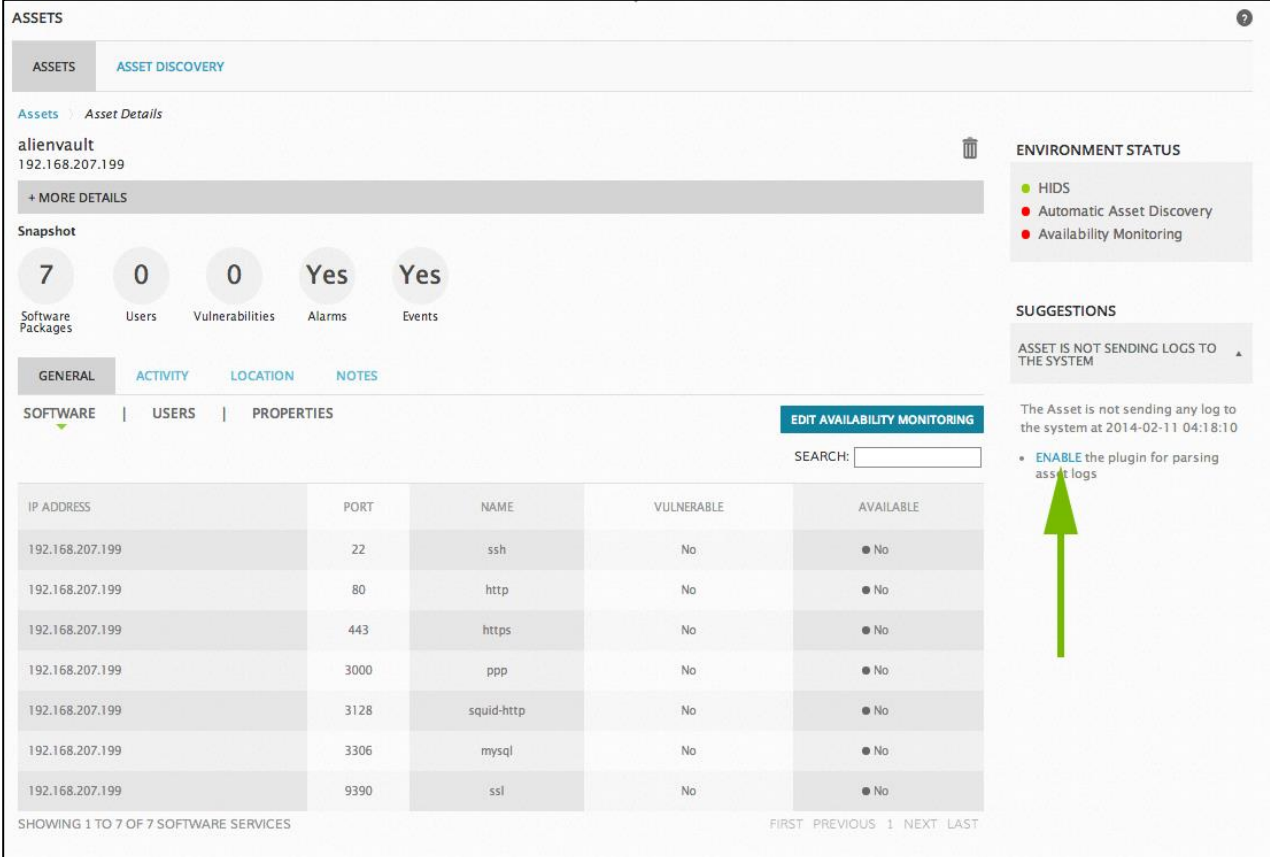
3. ENABLING DATA SOURCE PLUGINS

After configuring the external application or device to forward logs to an AlienVault Sensor (or All-in-One) the data source plugin must be enabled. This can be done through the web interface or through the command line console.

3.1. ENABLING DATA SOURCE PLUGINS IN THE ASSET DETAILS SCREEN

Navigate to “*Environment > Assets*” and view the details of an asset. The asset details screen shows info messages when an asset is not sending logs to the system:

Figure 1. Asset Details Screen



ASSETS

ASSETS ASSET DISCOVERY

Assets > Asset Details

alienvault
192.168.207.199

+ MORE DETAILS

Snapshot

7 Software Packages

0 Users

0 Vulnerabilities

Yes Alarms

Yes Events

GENERAL ACTIVITY LOCATION NOTES

SOFTWARE | USERS | PROPERTIES

EDIT AVAILABILITY MONITORING

SEARCH:

IP ADDRESS	PORT	NAME	VULNERABLE	AVAILABLE
192.168.207.199	22	ssh	No	No
192.168.207.199	80	http	No	No
192.168.207.199	443	https	No	No
192.168.207.199	3000	ppp	No	No
192.168.207.199	3128	squid-http	No	No
192.168.207.199	3306	mysql	No	No
192.168.207.199	9390	ssl	No	No

SHOWING 1 TO 7 OF 7 SOFTWARE SERVICES

FIRST PREVIOUS 1 NEXT LAST

ENVIRONMENT STATUS

- HIDS
- Automatic Asset Discovery
- Availability Monitoring

SUGGESTIONS

ASSET IS NOT SENDING LOGS TO THE SYSTEM

The Asset is not sending any log to the system at 2014-02-11 04:18:10

- [ENABLE](#) the plugin for parsing asset logs

Click on the **ENABLE** link:

Figure 2. Enable plugin for the asset

ENABLE PLUGIN FOR ASSET

Confirm the vendor, model and version of the device shown. Click the button to enable the data source plugin for this asset.

DEVICE	VENDOR	MODEL	VERSION
alienvault [192.168.207.199]	Select Vendor ▼	Select Model ▼	Select Version ▼

CANCEL

ENABLE

Select a vendor, a model and a version, then click on **ENABLE**.

Follow the link in the 'INSTRUCTIONS' column for instructions on how to configure the 3rd party device to forward logs to AlienVault.

Follow the instructions and verify that the 'receiving data' icon turns green indicating that logs are being processed by AlienVault

Figure 3. Enable plugin for the asset

ENABLE PLUGIN FOR ASSET

Plugin successfully configured. It can take up few minutes. Click on the instructions for each device for information on how to configure the device to send it logs to AlienVault. When AlienVault starts receiving data the light for receiving data will turn green.

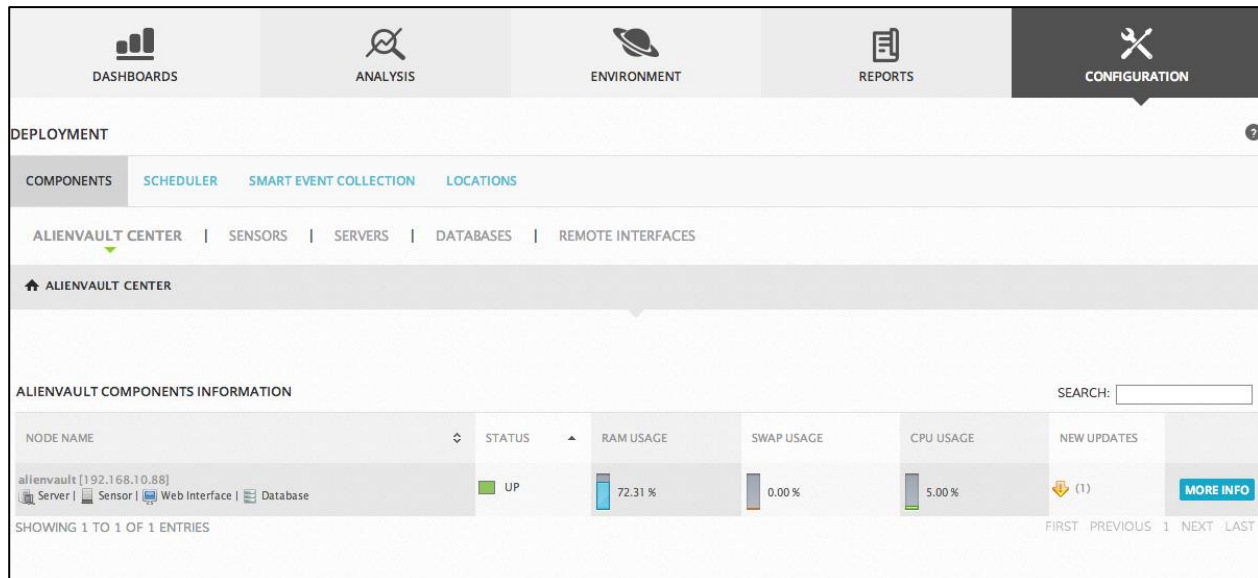
DEVICE	TYPE	INSTRUCTIONS	RECEIVING DATA
alienvault	Apache Software Foundation SpamAssassin	Instruction to forward logs	●

CLOSE

3.2. ENABLING DATA SOURCE PLUGINS IN ALIENVAULT CENTER

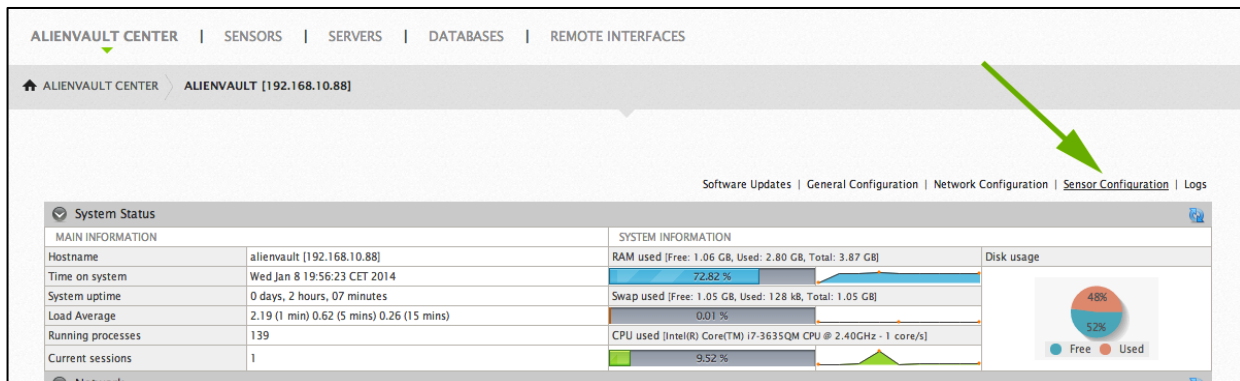
1. Log into your AlienVault Installation with a user who has administrative privileges
2. Navigate to "Configuration > Deployment".

Figure 4. Enabling Data Source Plugins In AlienVault Center: AlienVault Center



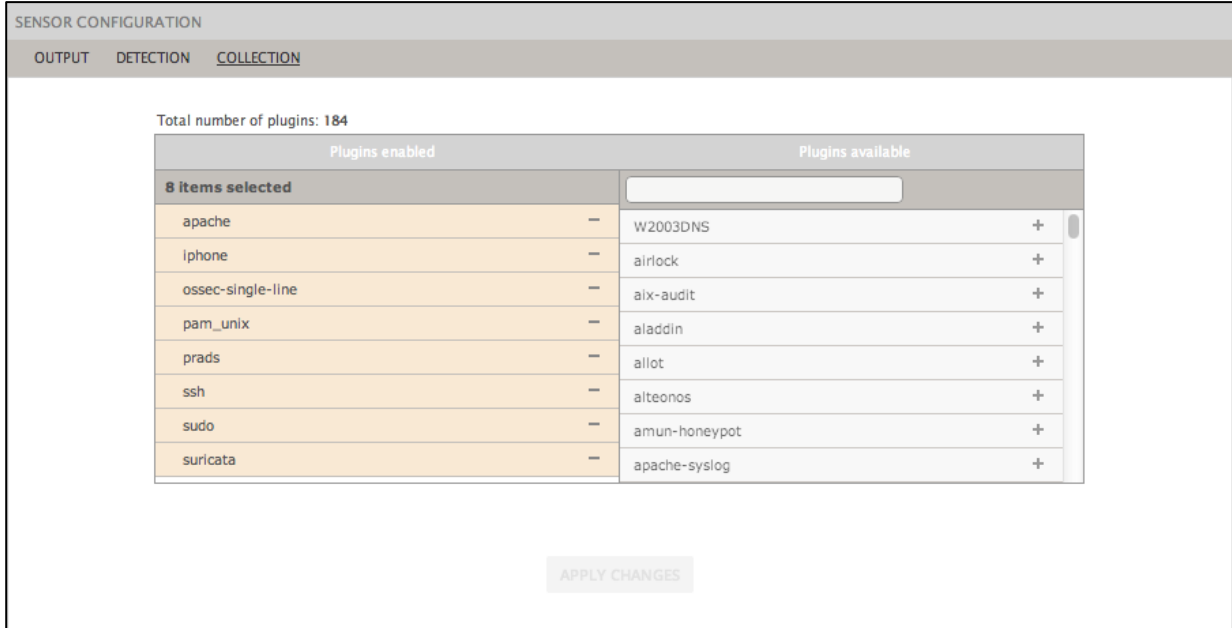
3. In the 'AlienVault Center Interface' select the row that corresponds to the AlienVault Component that was used in previous step 'Configure External Application or Device.'
4. In the detailed interface that corresponds to the component selected in the previous step, click on one on the **Sensor Configuration** link found at the top of the screen.

Figure 5. Enabling Data Source Plugins In AlienVault Center: "Sensor Configuration" Link



5. On the resulting screen, click on the 'Collection' link. The data source plugin configuration screen appears:

Figure 6. Enabling Data Source Plugins In AlienVault Center: enabled plugins



SENSOR CONFIGURATION

OUTPUT DETECTION COLLECTION

Total number of plugins: 184

Plugins enabled		Plugins available	
8 items selected		<input type="text"/>	
apache	—	W2003DNS	+
iphone	—	airlock	+
ossec-single-line	—	aix-audit	+
pam_unix	—	aladdin	+
prads	—	allot	+
ssh	—	alteonos	+
sudo	—	amun-honeypot	+
suricata	—	apache-syslog	+

APPLY CHANGES

This table displays 2 columns. The left column shows plugins that are enabled and the right column shows plugins that are available to be enabled.

To pass an item from one side to the other, drag and drop the item or use the links [+] or [-] which are next to each item.

6. To make all changes take effect, click the **APPLY CHANGES** button.

3.3. ENABLING DATA SOURCE PLUGINS THROUGH THE COMMAND LINE CONSOLE

1. Open a console terminal application and connect to the AlienVault System by running the following command:

```
ssh root@IP_address
```

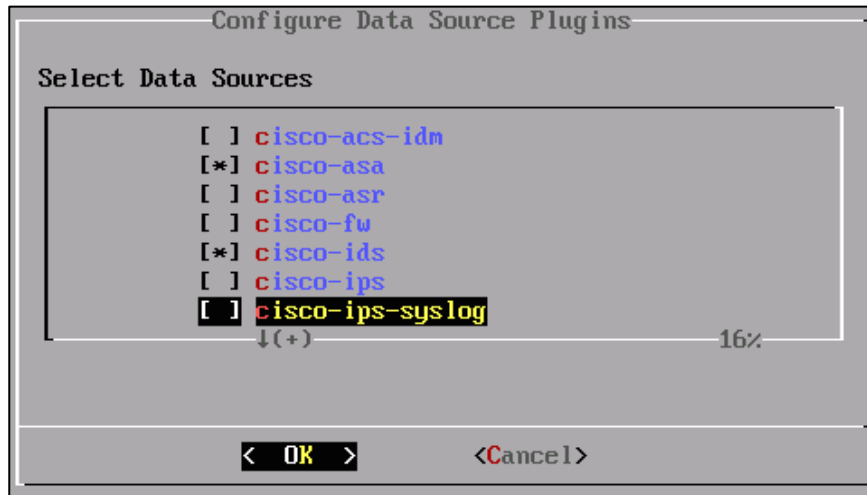
IP_address refers to the default IP of your appliance.

2. By using the arrow keys on the keyboard, select the option 1: “Configure Sensor”. Accept the selection (<OK>) by pressing **Enter** key.

To move from <OK> to <Exit> or vice versa, use the **Tab** key on the keyboard.

3. Select the option 4: “*Configure Data Source Plugins*”. Accept the selection (<OK>) by pressing **Enter** key.

Figure 7. Activate plugins by console: Select Data Sources



4. Select the plugins to activate. To move between them use the arrow keys on the keyboard and select/deselect it by pressing the **Space Bar** on the keyboard. It is possible to select several plugins. Accept the selection (<OK>) by pressing **Enter** key.
5. Navigate to the main menu by moving the cursor from <OK> to <Back> using the **Tab** key on the keyboard. Accept the selection (<Back>) by pressing **Enter** key.
6. Select the option 8: “Apply all changes”. Accept the selection (<OK>) by pressing **Enter** key.
7. Apply changes (<Yes>) by pressing **Enter** key.
8. The process can take several minutes depending on the number of plugins to activate

4. CONFIRM ALIENVAULT USM IS RECEIVING AND PRODUCING EVENTS

It is possible, through the web interface, check if a plugin is receiving events or not:

1. Log into your web interface
2. Navigate to “*Analysis > Security Events (SIEM)*”:



AlienVault Unified Security Management™ Solution

Data Source Plugin Management

3. Click on the combo of 'Data Sources' field and select the row corresponding to the Data Source Plugin that you just enabled.
4. Once a data source has been selected, confirm there are events displayed.

Figure 8. Security Events (SIEM) window: displayed events

The screenshot displays the 'SECURITY EVENTS (SIEM)' window. The interface includes a search bar, filters for 'SHOW EVENTS' (Last Day, Last Week, Last Month, Date Range), 'DATA SOURCES' (Directive_alert), 'RISK', 'SENSORS', 'TAXONOMY: PRODUCT TYPE', 'TAXONOMY: EVENT CATEGORY', 'IP REPUTATION ACTIVITY', and 'IP REPUTATION SEVERITY'. A 'SEARCH CRITERIA' section shows 'directive_alert' and 'Last Day'. The 'EVENTS' tab is active, showing a table of events. The table has columns for SIGNATURE, DATE GMT+1:00, SENSOR, SOURCE, DESTINATION, and RISK. The first four events are all 'directive_event: AV Policy violation, Dropbox file sharing service usage on 192.168.8.112', '192.168.12.60', '192.168.12.50', and '192.168.8.105' respectively, all dated '2014-01-08' and having a risk level of '1'. The table also shows '325 TOTAL EVENTS IN DATABASE'. At the bottom, there are buttons for 'INSERT INTO DS GROUP', 'DELETE SELECTED', 'DELETE ALL ON SCREEN', and 'DELETE ENTIRE QUERY'. A status bar at the bottom right indicates 'Priority threshold: 0', 'Active Event Window (days): 5', and 'Active Event Window (events): 4 M'.

SIGNATURE	DATE GMT+1:00	SENSOR	SOURCE	DESTINATION	RISK
directive_event: AV Policy violation, Dropbox file sharing service usage on 192.168.8.112	2014-01-08 19:34:37	N/A	Host-192-168-8-112:17500	255.255.255.255:17500	1
directive_event: AV Policy violation, Dropbox file sharing service usage on 192.168.12.60	2014-01-08 18:34:46	N/A	192.168.12.60:17500	255.255.255.255:17500	1
directive_event: AV Policy violation, Dropbox file sharing service usage on 192.168.12.50	2014-01-08 18:34:40	N/A	192.168.12.50:17500	255.255.255.255:17500	1
directive_event: AV Policy violation, Dropbox file sharing service usage on 192.168.8.105	2014-01-08 18:34:40	N/A	192.168.8.105:17500	255.255.255.255:17500	1



APPENDIX A - CONFIGURING ALIENVAULT TO RECEIVE LOGS THROUGH SYSLOG

Devices that send log data via Syslog require configuration of the Syslog service to process those incoming logs into a unique file destination.

1. Open the console on the AlienVault Appliance, or log in over Secure Shell (SSH) as “root” user.
2. Select and accept the “*Jailbreak this Appliance*” option to gain command line access.
3. Create a new configuration file to save incoming logs:

```
nano -w /etc/rsyslog.d/dataSource_name.conf
```

dataSource_name should be replaced with the file name of the Data Source.

4. Add the following line to the file, one for the device you are sending logs from:

```
if ($fromhost-ip == 'IP_Address') then /var/log/dataSource_name.log  
& ~
```

IP_Address should be replaced with the IP address of the device.

5. Press **Ctrl+W** to save the file and **Ctrl+X** to exit the editor.
6. Restart the Syslog Collector:

```
/etc/init.d/rsyslog restart
```

APPENDIX B - CONFIGURING LOG FILE EXPIRATION



This log must be configured if the data source plugin does not read events from syslog file.

Incoming logs are processed by the Sensor and passed on to the Server. Keeping the raw log files on the sensor for more than a few days is unnecessary and they should be purged to maintain adequate free file system capacity.

1. Create a new log rotation configuration file:

```
nano -w /etc/logrotate.d/dataSource_name
```

dataSource_name must be replaced by your data source file name.

2. Add the following content to the file:

```
/var/log/dataSource_location.log
{
    rotate 4 # save 4 days of logs
    daily # rotate files daily
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
        invoke-rc.d rsyslog reload > /dev/null
    endscript
}
```

dataSource_location must be replaced by the specified location in the data source plugin.



APPENDIX C - DEBUGGING CONNECTION FROM DEVICE TO ALIENVAULT

If the plugin is generating new logs, yet not appearing in the AlienVault SIEM Events UI (for example, the device is not listed as an available plugin); the following steps will assist in isolating at which stage of processing the logs are reaching before failure.

1. Log Events should begin to appear in the Web UI under “*Analysis > Security Events (SIEM)*”.
2. If they do not, first validate that you are receiving syslog packets from the source device. Open the console on the AlienVault Appliance, or log in over Secure Shell (SSH) as the “root” user.
3. Select and accept the “*Jailbreak this Appliance*” option to gain command line access.
4. Validate that you are receiving syslog packets from the source device by writing the following:

```
tcpdump -i eth0 -v -w /dev/null 'src <IP Address> and port 514'
```

(the count of captured packet should indicate logs being sent)

5. Press “*Ctrl+C*” to exit this tool when finished.
6. Restart the Syslog Collector and the Sensor agent:

```
/etc/init.d/rsyslog restart  
/etc/init.d/ossim-agent restart
```

7. Search for any errors regarding the plugin in the Agent Logs.

```
cat /var/log/ossim/agent* | grep plugin_id="1636"
```

8. Write exit and press “*Enter*” key to exit Jailbreak.



APPENDIX D - LIST OF INSTRUCTIONS FOR DATA SOURCE PLUGINS

Vendor	Model/Product	Version	Instruction Link
CISCO	ASA	-	https://alienvault.bloomfire.com/posts/661005
CISCO	PIX Manager	-	https://alienvault.bloomfire.com/posts/661011
CISCO	PIX Software	-	https://alienvault.bloomfire.com/posts/661011
CISCO	Wireless LAN Controller	-	https://alienvault.bloomfire.com/posts/600869
Citrix	NetScaler	-	https://alienvault.bloomfire.com/posts/601121
Dell	SonicWALL	-	https://alienvault.bloomfire.com/posts/596832
F5	Firepass	-	https://alienvault.bloomfire.com/posts/594271
Fortinet	Fortigate	300c-800c	https://alienvault.bloomfire.com/posts/594397
Imperva	SecureSphere	1.0-8.5	-
InterSect Alliance	Snare	-	-
McAfee	CyberGuard TSP	-	https://alienvault.bloomfire.com/posts/594306
Microsoft	IIS	7.5	-
VMware	ESXi	-	-