AlienVault Users Manual

AlienVault LC - 1901 S Bascom Avenue Suite 220 Campbell, CA, 95008 T +1 408 465-9989 info@AlienVault.com http://www.AlienVault.com

Juan Manuel Lorenzo (jmlorenzo@AlienVault.com)

version 1.0

Table of Contents

Welcome to AlienVault!

Introduction

This manual contains configuration and operation guidelines to assist you with implementing and using our AlienVault SIEM.

As the de facto standard in the world today, AlienVault has a large community of users with experience using AlienVault SIEM in numerous types of applications ranging from compliance to operations, government to control systems, finance to manufacturing. This community of active developers and users communicate through the forums found on AlienVault's web site (http://www.alienvault.com). We encourage our customers to engage with this rich source of tactical expertise.

Since AlienVault SIEM is a fully unified security management system you will find a great number of tools you are familiar with already integrated into the AlienVault technology. These tools are not only manageable through the AlienVault interface but, they are also tightly integrated with the other functional components of the system. AlienVault products additionally integrate with external security tools of all sorts to allow you to create a unified solution to fit your specific needs. AlienVault is stands behind the technology we create. As a company with roots in the Open Source community we understand the necessity for honesty and transparency. This is critically important when it comes to addressing the types of integration SIEM users undertake. The AlienVault team delivers the same level of commitment to its community that has led the technology to be adopted by more than half of all SIEM users worldwide.

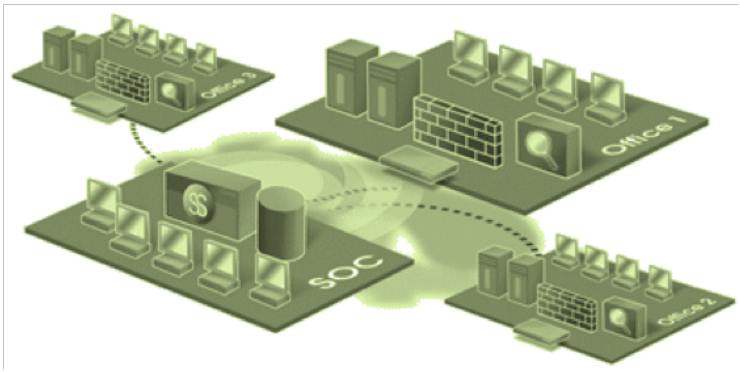
If you have any comments or questions about AlienVault and its products please contact us at any time.

Welcome to the AlienVault community!

What is AlienVault Unified SIEM?

AlienVault provides a Security and Event Management solutions, whose framework allows tight control over widely distributed enterprise networks from a single location.

The AlienVault Unified SIEM is created and developed by AlienVault.



AlienVault SIEM Technology offers advanced intelligence, capable of synthesizing the underlying risks associated with complex distributed attacks on extensive networks.

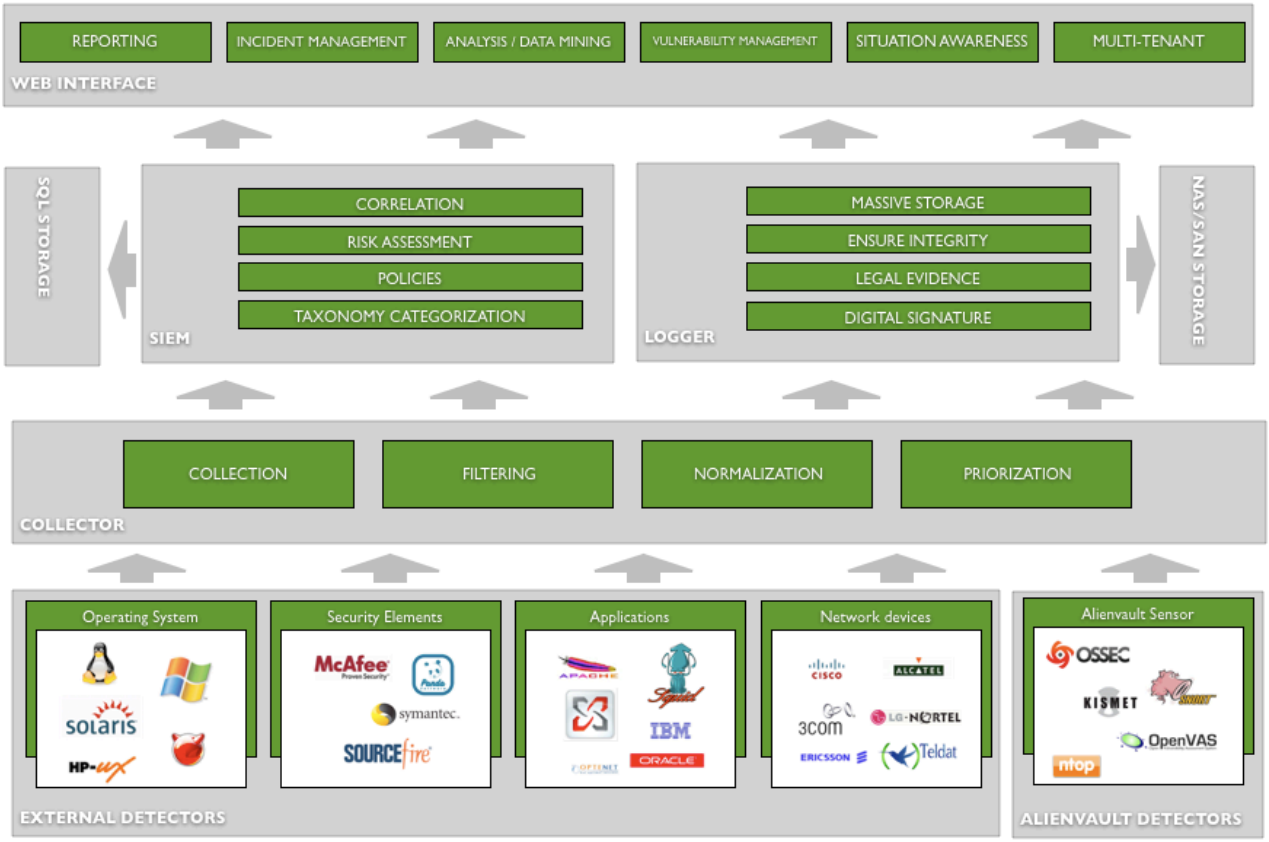
The system considers the context of each threat and the importance of the assets involved, evaluates situational risk, discovers, and distinguishes actual threats from the thousands of false positives that are produced each day in each network.

- The solution features:
- Low level, real-time detection of known threats and anomalous activity
- Compliance automation
- Network, host and policy auditing
- Network behavior analysis and situational behavior
- Log management
- Intelligence that enhances the accuracy of threat detection
- Risk oriented security analysis
- Executive and technical reports
- A scalable high performance architecture

Basic Operation

The following processes take place within AlienVault Unified SIEM:

- External applications and devices generate events (**External Data Sources**)
- Applications shipped with AlienVault generate events (**AlienVault Sensors**)
- Events are collected and normalized before being sent to a central Server (**AlienVault Sensors**)
- The AlienVault Server does the Risk Assessment, correlation and storage of the events in an SQL Database (**SIEM**)
- The AlienVault Server stores the events (Digitally signed) in a Massive Storage system, usually NAS or SAN (**Logger**)
- A web interfaces allows provides a reporting system, metrics, reports, Dashboards, ticketing system, a vulnerability Management system and real-time information of the network. (**Web interface**)



Components

Data Sources

Any application or device that generates events within the network that is being monitored will be considered a Data Source within the AlienVault deployment.

AlienVault includes a number of Data Sources using well-known Open Source Tools. From this moment we will use AlienVault Data Sources when referring to the Data Sources included by default when installing AlienVault Unified SIEM.

AlienVault Sensors have been designed for managed security. They compile an arsenal of technology into a single device, and introduce it into each remote network as if it were an “eye” detecting unauthorized activity. The combined result of numerous detection and control points is global visibility and compliance management.

AlienVault Sensors are installed on each network segment and inspect all traffic, detecting attacks through various methods and collecting information on attack context without affecting network performance.

These sensors utilize more than 10 expert systems that identify attacks along 5 different axes:

- Intrusion Detection
- Anomaly Detection
- Vulnerability Detection
- Discovery, Learning and Network Profiling systems
- Inventory systems

Detection systems locate in near real time, both known and unknown attacks through learning and anomaly reporting.

The Vulnerability detection system discovers and identifies latent network threats and can correct them before an attack occurs. This information, stored by the Management Server, is of vital importance when an attack is in progress. Prior knowledge of vulnerabilities in systems is vital when assessing the risk associated with an attack, prioritizing, alerting, and launching countermeasures.

The network information gathered by AlienVault probes also provide detailed information in near real time about network usage of each computer, which it then collects for analysis. The system automatically creates a highly detailed usage profile of each element on the network.

Sensor

The Sensors gather the events generated by external Data Sources and by Data Sources running within the AlienVault Sensors. Sensors classify and normalize the events before sending them to SIEM and Logger.

In order to support the maximum possible number of applications and devices, Sensors use Data Source connectors (also called Collection Plugins). Each DS connector (Formerly AlienVault Plugins) define the way events generated by each detector should be collected and normalized.

DS connectors can be configured easily using a simple configuration file and regular expressions to define the format of each type of event.

The Sensor component can be deployed as a standalone system or included in the Sensor or SIEM appliance depending on your needs.

SIEM

The SIEM component provides the system with Security Intelligence and Data Mining capacities, featuring:

- Risk assessment
- Correlation
- Risk metrics
- Vulnerability scanning
- Data mining for events
- Real-time monitoring

AlienVault SIEM uses a SQL database and stores information normalized allowing strong analysis and data mining capacities.

AlienVault Unified SIEM is tuned for high performance and scalability of millions events per day.

Logger

PRO ONLY

The Logger component stores events in raw format in the file system. Events are digitally signed and stored en masse ensuring their admissibility as evidence in a court of law.

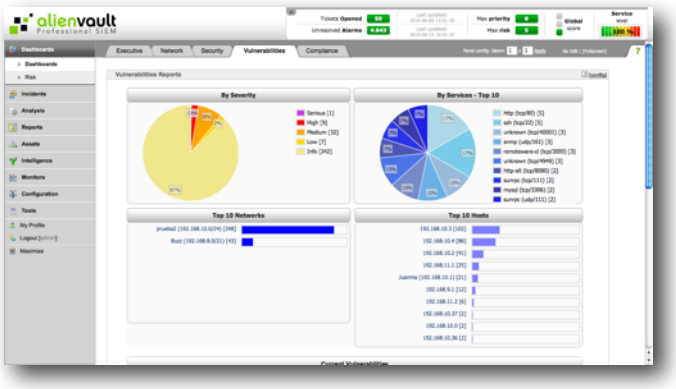
The logger component allows storage of an unlimited number of events for forensic purposes. The logger is usually configured so that events are stored in a NAS / SAN network storage system.

Web interface

The Web interface provides access to all information collected and generated by the system as well as access to the configuration parameters.

The following tasks can be performed using the Web interface:

- Configuration changes
- Access to Dashboards and Metrics
- Multi-tenant and Multi-user management
- Access to Real-time information
- Reports generation
- Ticketing system
- Vulnerability Management
- Network Flows Management
- Responses configuration



AlienVault Web interface

Introduction

The AlienVault Web interface displays all the information collected and generated by AlienVault products. The web interface provides access to the information stored in both SIEM and Logger. The Web interface also provides real-time information on the status of the monitored networks as well as the possibility of configuring the AlienVault deployment.

Access the AlienVault Web Interface

To access the AlienVault Web Interface point your browser to the IP address of the machine that has in which you have installed the Web Interface profile (Formerly known as Framework). If you have installed a single AlienVault box point your browser to the IP address of that box.

http://IP_ADDRESS_OF_THE_AlienVault_BOX

Login

To access the AlienVault Web interface enter a user and a password and click on Login. If you want to login and open a maximized window displaying the AlienVault Web interface mark the checkbox next to Maximized.

Default User - Password

AlienVault is installed by default with a single user. This user will always keep special permissions within the AlienVault system (Permissions to monitor all assets and all menu options enabled).

The default user is ***admin*** *with* ***admin*** as password. As soon as you log in to the system you will be prompted to change the password.

Reset Default User - Password

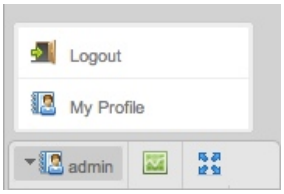
If you forget the admin password you can reset the password using the following command in the linux console.

AlienVault-reset-password admin

This command can be used to change the password of any user from the console. Anyway, an administrator user will always be able to change the password of another user using the AlienVault Web Interface.

Logout

User sessions will finish automatically after some time. If you want to logout manually click on the name of the user at the bottom of the left menu and then click on **Logout**.



Dashboard

Dashboards

Dashboards

Dashboards -> Dashboards

Description

The Dashboards tab allows each user on AlienVault set up their personal configuration of charts and indicators to show all the information collected and generated by AlienVault. When creating a new user in the AlienVault Web interface it is possible to assign the admin user dashboard as the default dashboard for the new user.

The Dashboard is divided into different tabs; each tab has a different window. The user can define the content of each window using the configuration wizard.

By default, the dashboard includes several tabs designed by the AlienVault team. Each user can customize his dashboard using the predefined tabs and windows as reference or even create their own panel from scratch.

Tabs

The Dashboards panel includes the following tabs by default:

Tab	Content
Executive	High level metrics and information
Network	Network Statistics (Ntop & Aggregated Risk)
Tickets	Ticketing system statistics
Security	Statistics and Reports on SIEM Events
Vulnerabilities	Vulnerability Scanning Reports
Inventory	Statistics and reports on the OCS and AlienVault inventory
Compliance	Compliance Report Graphs

Windows

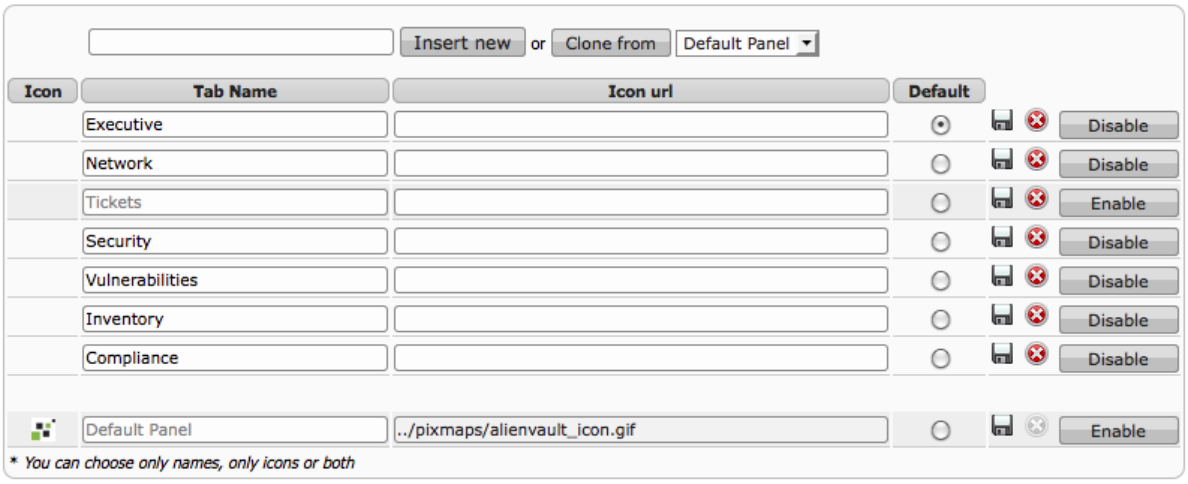
Each tab contains many different Windows. The number of windows shown in each tab can be customized. The user will configure the content of each window using one of the following plugins:

- RSS Feed
- Custom Tag-Cloud
- Config Import
- Metrics Metapanel
- Custom HTML contents
- Custom SWF graph
- Custom SQL graph

Usage

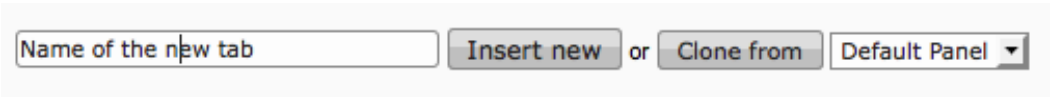
Edit Tabs

To edit the tabs just click on **Edit tabs** in the upper right corner. There you will find a list all tabs (Enabled or disabled). The tabs that come by default when installing AlienVault can not be deleted, they can only be disabled. You can also use those tabs as a template to create your own tab. Default tabs can be identified because they have the AlienVault icon next to their names.



New Tab

To create a new tab, enter the name of the new tab, and click on **Insert New**. If you want to use one of the default panels as template, select one from the drop box and click on **Clone from**.



Delete Tab

To delete a tab, click on this icon in the line of the tab that you wish to delete.

Modify tab

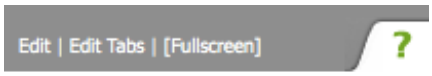
After modifying the name or the icon of the tab you will have to click on this icon to save changes.

Default tab

To select which tab will be shown by default, mark the checkbox (Default column) of the tab that you want to see as Default panel.

Geometry

To modify the Geometry of each tab, click on **Edit** in the upper right corner



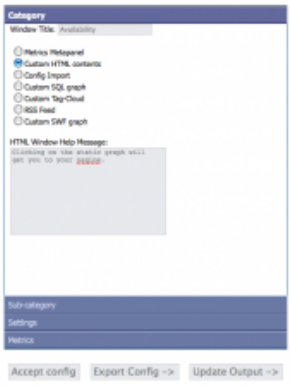
Now you can configure the number of rows and columns that will be shown in this tab.

To save the new geometry of the tab click on **Apply**

Edit Windows

To customize the content of each window you must be in edit mode, click on **Edit** in the upper right corner of the Dashboard panel and then click on '**config**' in the upper right corner of the window you want to edit.

This enters you into the edit mode of the window. You will find the configuration on the left side and the preview of the window on the right side, to update the preview click on **Update Output**. Once you have finished configuring the window click on **Save Config**.



Risk

Maps

Dashboards -> Risks -> Risk Maps

Description

Risk Maps allow visualization of the status of any object (Hosts, Host groups, Networks, Network groups) being monitored by AlienVault. Both maps and icons that represent each object on the map can be customized.

Linking maps allows the user to create different levels of visualization, reaching the lowest possible level (Eg: Server Racks) or up to a global view showing the different locations of the company that is being monitored around the world.

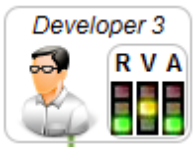
Users in AlienVault with permissions to see this tab will see all maps, but they will only see those objects that they are allowed to monitor, all of which is based on their user permissions.

Maps

AlienVault includes several maps by default. In addition to these predefined maps, each user can upload their own images (photographs, maps, network …) to set the indicators that represent the different objects in the network that are being monitored by AlienVault.

Indicators

Every object in the AlienVault inventory is plotted on the map with an indicator, each indicator includes an icon that allows the user to visually identify the object being monitored.



Each indicator provides information about the Risk (**R**), Vulnerability (**V**) and Availability (**A**) status of each object located on the map.

Risk

The risk indicator shows the risk value of the object by relating compromise and attack values with the compromise and attack threshold defined within the AlienVault inventory for that object.

Vulnerability

The indicator for the level of vulnerability is calculated based on the results of vulnerability scans performed by the vulnerability scanner (OpenVas or Nessus) using the AlienVault interface.

The system gets the risk value of the most serious vulnerabilities of the object, the vulnerability status will be yellow whenever there is a vulnerability with a risk greater than 3, and red when the risk is higher than 7. If the host has no vulnerabilities, no vulnerability scans have been done, or the risk of the vulnerabilities is lower than 3, the vulnerability status will be displayed with a green icon. This indicator will only be useful whenever the host and networks are being analyzed by the Vulnerability Scanner (Nessus or OpenVas).

Availability

The availability indicator is calculated using the information collected from Nagios (the availability monitor in AlienVault). This indicator will only be useful whenever the host and networks are being monitored by Nagios.

Usage

Maps

You can use any image or photograph as a map. As an example, it is possible to have indicators providing information on the status of the servers, placed in a photo of a rack. It is also possible to use a world map and integrate the various indicators that provide information on network that the corporation that is being monitored has deployed in each country.

Upload a map

You can use any file in (.jpg, .png, and .gif format) as a map. The maximum size of the image is 2MB. As for the size of the image, this will depend largely on the resolution of the screen that will be displaying the map.

To upload a new map, click on Manage Maps and then use the form to select the file that you want to upload, and click on **Upload.**

Select default map

The default map will be displayed whenever the user gets into Dashboard → Risk Maps. To select the default Map click on **Manage Maps** and click on **Set as Default** under the map that you want to set as default map.

Delete a map

To delete a Map, click on Manage Maps and click on the red [X] under the map that you want to delete.

Indicators

Each indicator will show the status of the different objects defined within the AlienVault inventory. If you want to show the status of an object that does has not been included in the AlienVault inventory, you will have to insert in Assets → Assets.

New indicator

To place a new indicator in the Map, first you'll have to select the map in which you want to insert the new indicator clicking on Manage Maps and then clicking on the desired Map.

Once the Map that you want to modify is displayed, click on Set Indicators. In the left side you will find a box in which you will have to configure the new indicator that will be displayed on the Map. Before inserting the new indicator in the map, select the icon that will identify the object clicking on **Choose from List**. Depending on the background image you may want to configure the background color of the indicator to be white or transparent using the Background drop menu.

After configuring the icon that will be displayed within the indicator, you will have to select the object of which status is shown.

A name has to be assigned to each indicator before clicking on **New indicator**. When the indicator is displayed on the map the user can click on it, so you can link the indicator to any URL, to the Host/Network report in AlienVault and to another map. When linking an indicator to another map, you will be able to create different views of the status of your corporation, from a global view up to the view of the status of every host in the local network of one of the locations.

To place the indicator in the map click on **New indicator**. The new indicator will appear in the upper left corner of the map.

Move indicators

To move an indicator just click and hold on the indicator, move the indicator to the desired location and click on **Save Changes** in the left menu.

Modify indicators

To modify an indicator just click on the indicator, the left side menu will allow you to change the icon, name, position, and the URL the indicator will link to.

Delete indicators

To delete an indicator just click and hold on the indicator and move it to the trashcan icon that appears in the upper left corner on the map.

Icons

Icons help identify the object that is being shown in the indicator. A set of icons are included by default with AlienVault, but each user can use their own icons to identify the hosts and networks that are being displayed in each map.

Upload Icons

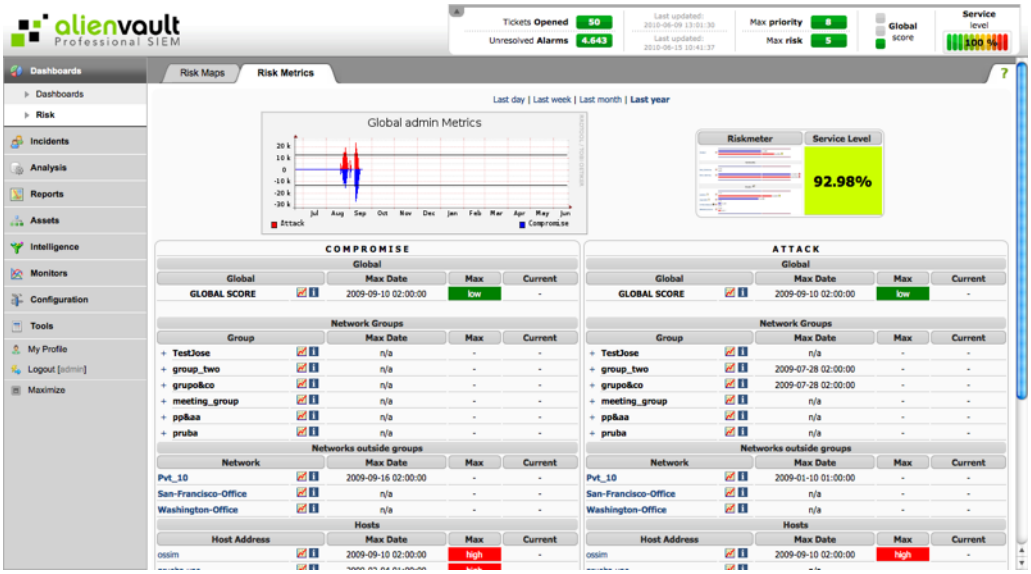
To upload a new icon, click on **Set Indicators** and in the left menu use the form on top writing the name of the new icon and browsing an image in your system in .gif, .png, or .jpg format. The image should have a maximum width and height of 50 pixels. Click on **Upload** to upload the new icon. To use the new icon, you will have to select the **Own uploaded** category when selecting the icon of the indicator.

Metrics

Dashboards -> Risks -> Risk Metrics

Description

The Aggregated Risk panel provides a graphical representation or dashboard of the global impact of system level attacks.

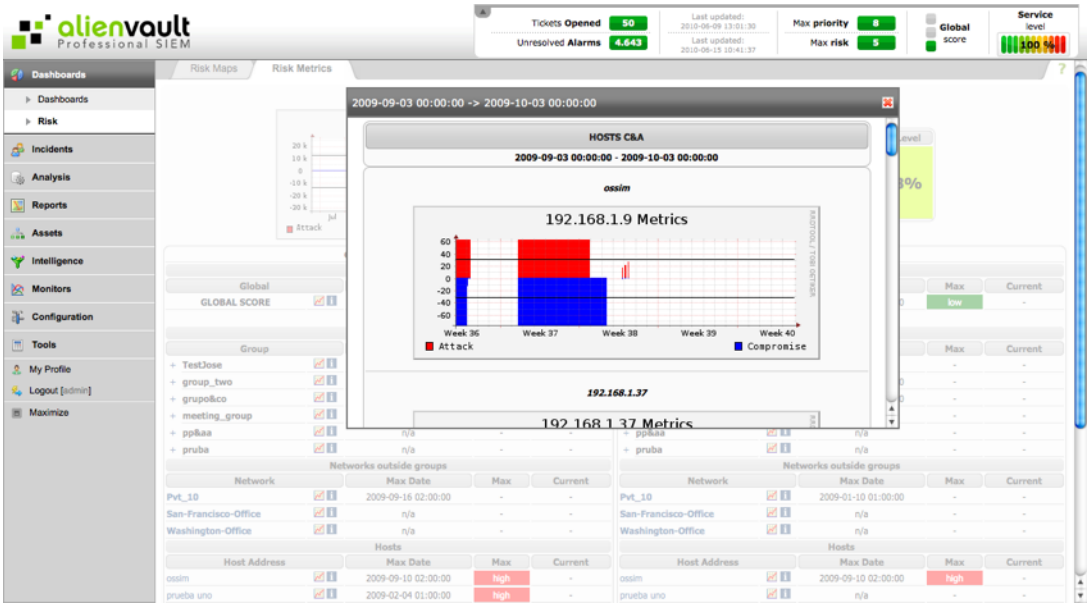


"Attack" and "Compromise" are a set of indicators of aggregated risk. Within these categories are global metrics that reflect the security impact of events on monitored assets. "Attack" represents the potential machine risk due to attacks on the organization's systems. It is a measure of the degree of risk from active attacks, but does not actually indicate that any of the attacks have been successful. The "Compromise" section indicates that an attack was successfully committed against a machine.

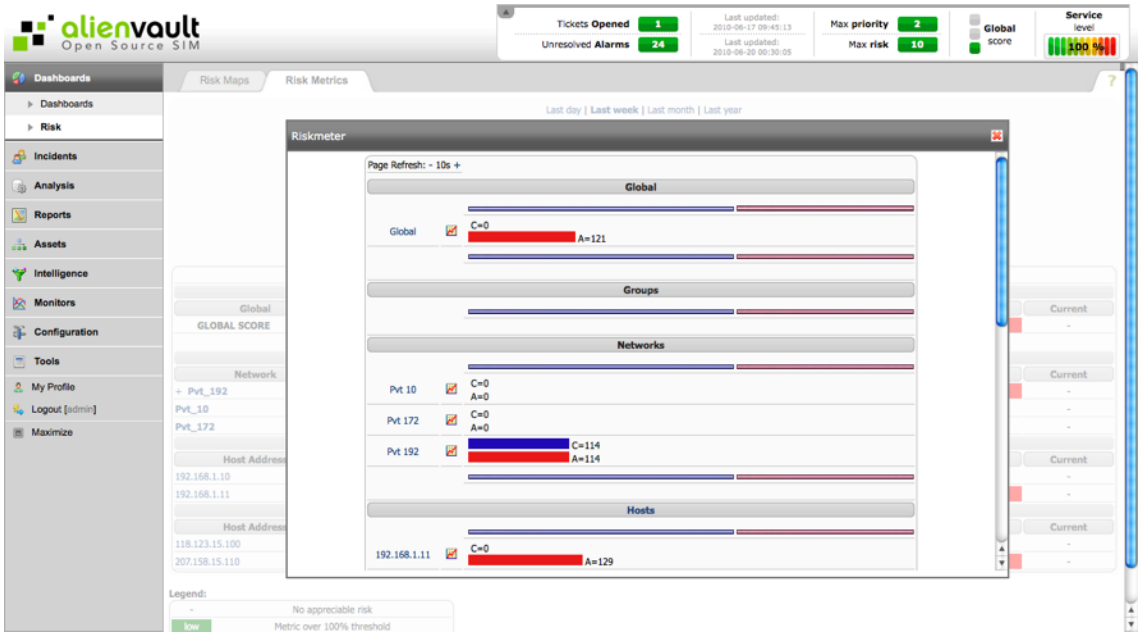
The Metrics page is organized into four sections:

- The top panel lets you select the duration of your metrics: over the last 24 hours, the last week, month, or year.
- The middle panel provides a graphical representation, or dashboard of Global Administrative Metrics, a Risk Meter, and Service Level.
- The bottom left panel provides Compromise information.
- The bottom right panel provides Attack information.

Clicking on the Global Admin Metrics graph (Blue or Red part) will cause it to appear in a new window for easier viewing. This graph displays instances of attacks and compromised systems at the specific time and date in which the events occurred.



Clicking on the “Risk meter” graph will also cause it to appear in a new window. It is a real time monitor of system risk on a global, network, and host scale.



The “Service level” graphic displays the current service level of your systems and networks. This information is derived from the same information sources as the “Risk meter”. You can click the displayed percentage, view related admin metrics, and modify the duration of time displayed in the graph (past day, week, month, or year), or whether or not to show attacks or compromises.

The information displayed in the Compromise and Attack section in the bottom panel displays is similar for both categories. Events are divided into three types: global, network groups, and networks outside groups. The Global section contains four pieces of information: the Global Score, the maximum date, the maximum and current levels. The Global Score features two icons: a graph and an information symbol. By clicking the graph symbol, the Global admin Metrics window appears, exactly like the one in the top panel. The Information icon allows you to configure settings for the incident metric, allowing you to insert the associated data into a new incident. You can modify suggested information, if needed. For example, you can apply a title to the incident, set its priority, type, target, metric type and value, as well as beginning and end times of related events.

Each user will see information in this screen based on the objects this user is allowed to monitor.

Risk calculation

In AlienVault a risk value (0-10) is calculated for every event once it arrives to the AlienVault SIEM. We can avoid this risk calculation using Policies.

The following formula is used to calculate a risk for every event:

(ASSET VALUE * PRIORITY * RELIABILITY) / 25 = RISK OF THE EVENT

The variables can get the following values:

(ASSET VALUE(0-5) * PRIORITY(0-5) * RELIABILITY(0-10)) / 25 = RISK OF THE EVENT (0-10)

Asset Value

Each Asset in AlienVault (Host, Host Groups, Networks and Network Groups) will have an asset value (0-5). Each object will have a different value in each network.

As an examples printers may not be important in some corporation (Asset Value 0 or 1), but they may be so important in a different corporation in which printers are the most important asset on their network.

When calculating a risk for an event in AlienVault, we may find some events with two hosts involved in generating the event. In that case we will use the highest Asset Value.

If the host that has generated the event is not defined within the AlienVault inventory the system will use 2 as default Asset Value.

When doing the risk calculation the system will try to get the asset value of the host, if the host has not been included in the AlienVault inventory the system will check whether the host belongs to one of the defined networks. If the host belongs to one of the networks and the host has not been defined by itself the system will use the network Asset Value to do the risk calculation.

Priority

Priority is the importance of the event itself; it is a measurement which is used to determine the relative impact an event could have in our network.

Priority is a value between 0 and 5

- **0** No importance
- **1** Very Low
- **2** Low
- **3** Average
- **4** Important
- **5** Very Important

Reliability

Reliability determines the probability of an attack being real or not. We are not determining if the event is a false positive or not (E.g.: A single authentication failure event it is not a false positive, but I cannot confirm that the corporation is undergoing a brute force attack with a single event).

Reliability can be a value between 0 and 10

- 0 False Positive
- 1 10% chance of being an attack
- 2 20% chance of being an attack
- …
- 10 Real attack

Aggregated Risk

An aggregated risk is calculated for every object (Hosts, Host groups, Networks and Network groups) belonging to the AlienVault Inventory using two indicators (the compromise and the attack value).

This two indicators will help us identify whether an object in our network may have been compromised (It is attacking other hosts or networks) or is under attack.

Compromise

Compromise means a network element is generating lots of events (as source), this is, it's behaving like if it's been compromised. Compromise is calculated by taking into account the risk for all the elements where the specific element is involved as source.

The compromise value is increased based on the risk of the event calculated using the asset value of the source of the event. The system will increase the compromise value of the host, of the networks and host groups the host belongs to, and of course the global compromise value.

Attack

Attack is a value that measures the level of attack an element has received in our network, that is, how much it has been attacked.

In order to determine the attack level for any network element, the risk value of all the events where the element is involved as destination is added.

The attack value is increased based on the risk of the event calculated using the Asset value of the destination of the event. The system will increase the attack value of the host, of the networks and host groups the host belongs to, and of course the global compromise value.

Threshold

Depending on the amount of collected events and the risk of those events each corporation will have a different compromise and attack value. You will have to update the threshold to tell the system what you consider a normal situation in your corporation. This tuning should be done whenever you have integrated all devices in AlienVault and when nothing strange has happened in your network (No attacks, no new devices, and no availability problems).

To adjust the global Threshold, use the parameter **Global Threshold** in Configuration → Main → Metrics. Apart from this global threshold each object will have its own Compromise and Attack Threshold that will be set in Assets → Assets.

Recovery

Events will increase the Compromise and Attack values but none of them will decrease the value, so the system will automatically subtract a value every 15 seconds.

This value is stored in the parameter **Recovery Ratio** in Configuration → Main → Metrics

Incidents

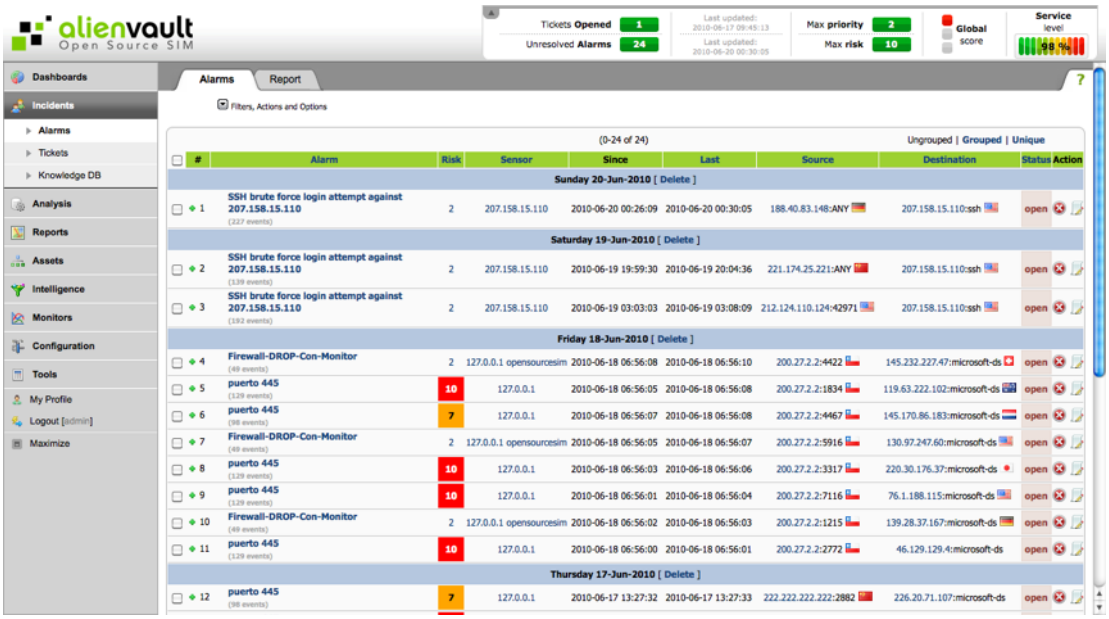
Alarms

Alarms

Incidents -> Alarms -> Alarms

Description

The Alarm Panel shows all the alarms generated in AlienVault. Each user will only see the alarms belonging to the hosts that they are authorized to monitor based on the user permissions.



Alarm

An alarm is an event that has a risk higher than 1. Alarms are a special type of event since it may group more than one event when the event becomes an alarm generating using correlation directives.

The correlation engine will only generate new events, that may become alarm or not, when risk is calculated for the new event. An alarm can also be generated with a single event if the event has high priority and reliability values and the value of the hosts involved in generating the event is high enough.

Usage

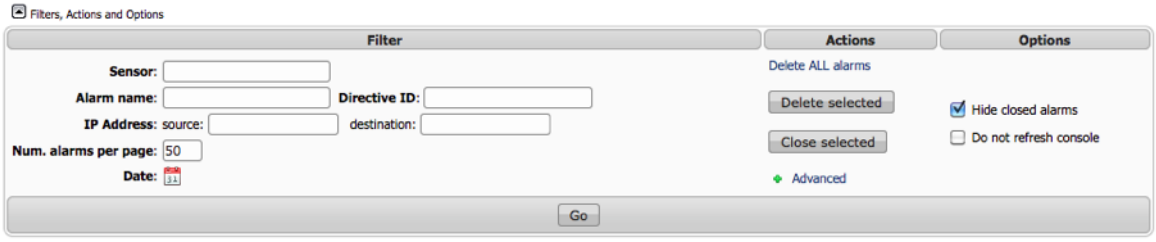
Alarm View

The default Alarm View will show the following columns:

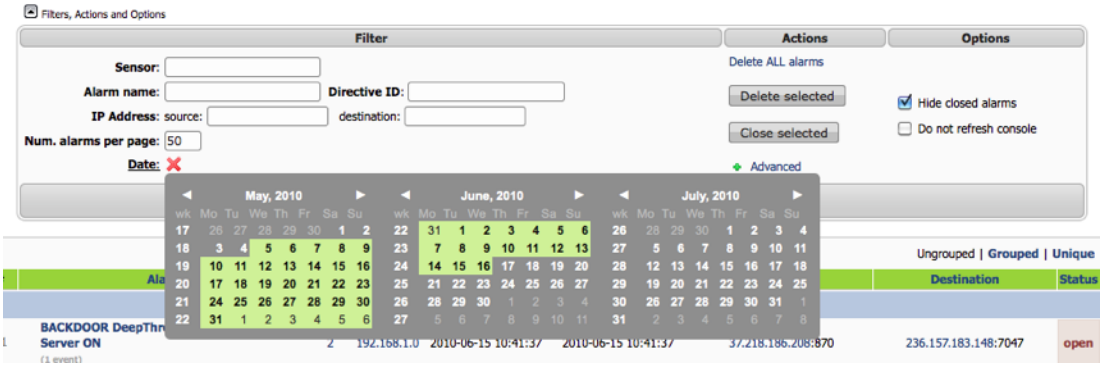
Column	Content
Alarm	Name of the alarm: Name of the directive for events generated during Correlation or Name of the event when a single event generates an alarm
Risk	Risk Value from 0 to 10
Sensor	Sensor that has collected the events generating an alarm (Events generating an alarm may have been collected by more than one sensor)
Since	Date and time of the first event belonging to the alarm
Last	Date and time of the last event belonging to the alarm
Source	Source of the event or events generating the alarm (May be more than one source but only the first will be shown)
Destination	Destination of the event or events generating the alarm (May be more than one destination but only the first will be shown
Status	Status of the alarm: Open or Closed

Filters

To filter or show only certain alarms click on **Filter, Actions and Options** in the upper left corner. This will display the following form:



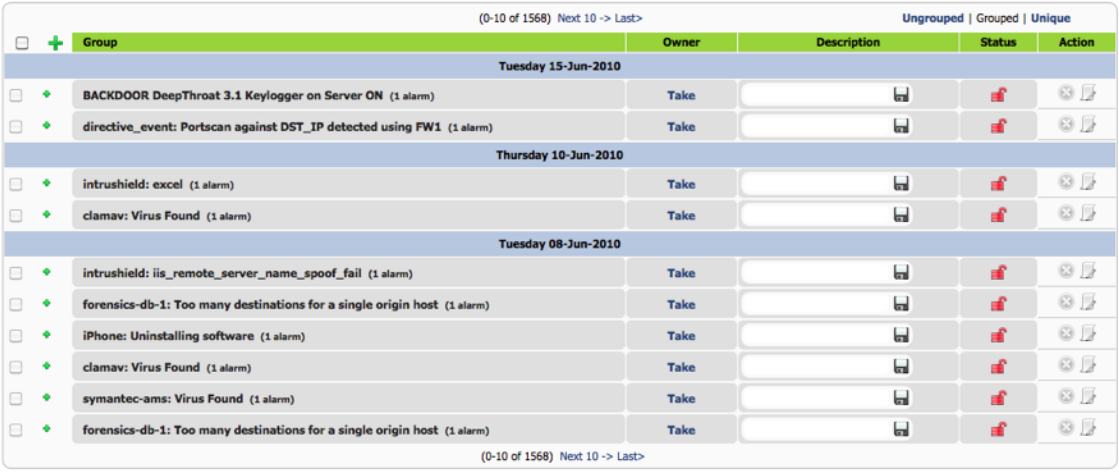
This form allows filtering based on Sensor, Alarm Name, Source and Destination. Alarms can also be filtered based on the time range in which they were generated using the following calendar:



The number of alarms displayed per page can also be configured using the parameter **Num. alarms per page**. The system will show 50 alarms per page by default.

Grouped Alarms

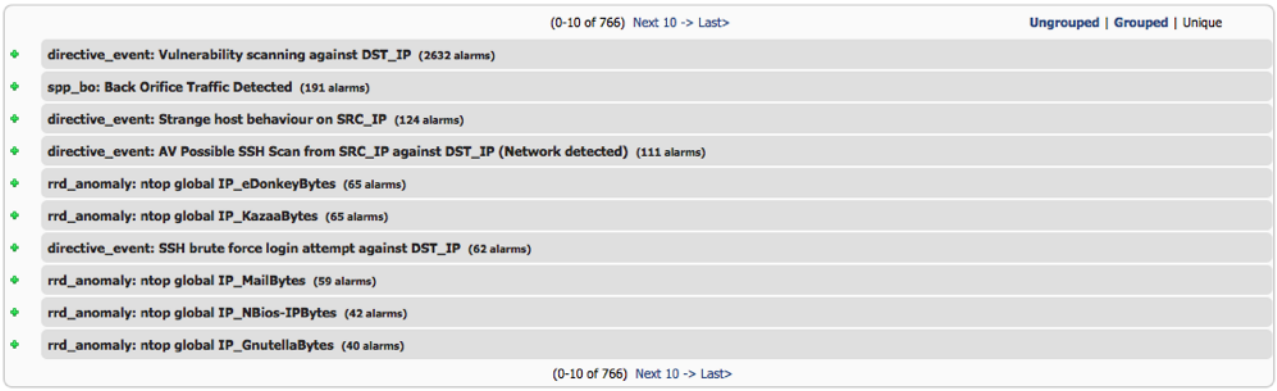
To simplify the analysis of the alarms, alarms can be grouped based on the type of alarm, the source and the destination. To access the grouped view of the alarms click on **Grouped** in the upper right corner.



A correlation directive that is not grouping enough events may be generating the same alarm many times, with the same source and same destination in a short period of time. To avoid this we will have to modify the correlation directive.

Unique Alarms

The Unique Alarms view will group all alarms by type of alarm, to access this view click on **Unique** in the upper right corner.



Manage Alarms

Close Alarms

Closed Alarms will not be shown in the Web interface by default. Once an alarm has been analyzed it should be closed. This way it will be easier to manage future alarms.

Some reports such as the compliance reports use the alarms (Closed or opened) to generate the reports, for this reason alarms that have not been deemed a false positive should never be deleted, they should just be closed.

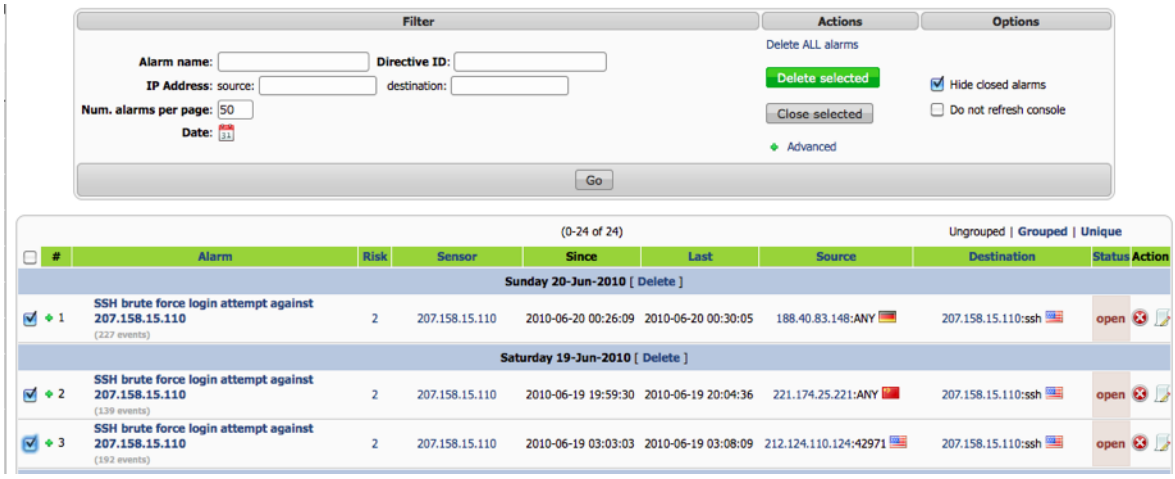
To close an alarm click on this icon  next to the alarm that you want to close, to see both opened and closed alarms, click on Filters, Actions and Options and unmark the checkbox next to **Hide closed alarms**.

To close more than one alarm click on **Filters, Actions and Options**, mark the checkbox next to the alarms than you wish to delete and then click on **Close selected**.

Delete Alarms

Only alarms that have been considered a false positive should be deleted. Alarms representing a real problem in the network should be closed nor deleted. You can delete all alarms that happened the same day by clicking on Delete next to the date:

To delete more than one alarm click on **Filters, Actions and Options**, mark the checkbox next to the alarms than you wish to delete and then click on **Delete selected**.



Analyze Alarms

Detailed View

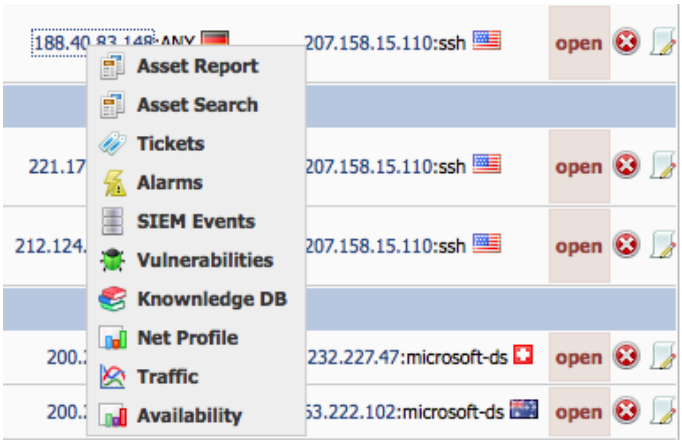
When a correlation directive is generating events, all the events will be grouped within the same alarm. In this case the alarm will be composed of many different types of events. To see all those events click on the green cross next to the alarm name:

This will display a new window with all the events organized by the correlation level in which the events have been collected:

Clicking on each event will show the original event in the forensic console.

Right click View

Right clicking on any IP address will show a menu that provides direct access to all the information stored by the system for that specific IP address as shown in the following image:



New ticket

To open a new ticket in the ticketing system from an alarm, click on this icon  next to the alarm.

Report

Incidents -> Alarms -> Report

Description

This page shows graphs and charts generated based on the data of the alarms generated within AlienVault.

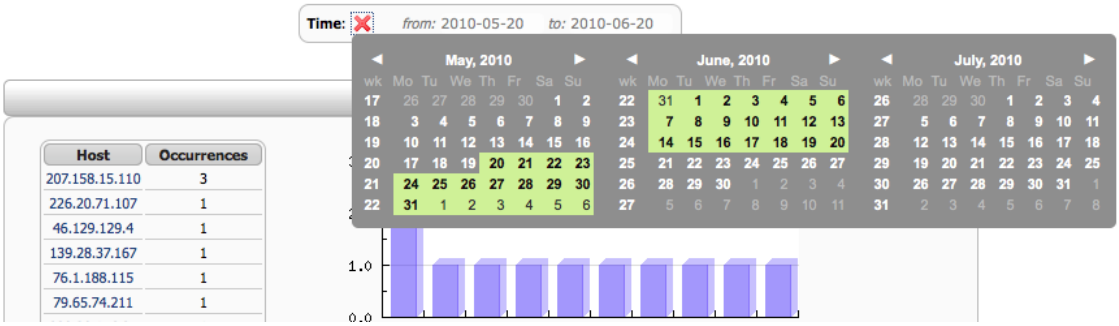
Usage

This page features the following charts:

- Top 10 Attacked Hosts
- Top 10 Attacker Hosts
- Top 10 Used Ports
- Top 10 Alarms
- Top 10 Alarms by Risk

With the exception of the final chart, Top 10 Alarms by Risk, you can find more information about the hostname, alarm, or port by clicking its corresponding link.

To modify the time range used to generate the report click on this icon  and select the time range you want to use as source of information to generate charts and graphs.



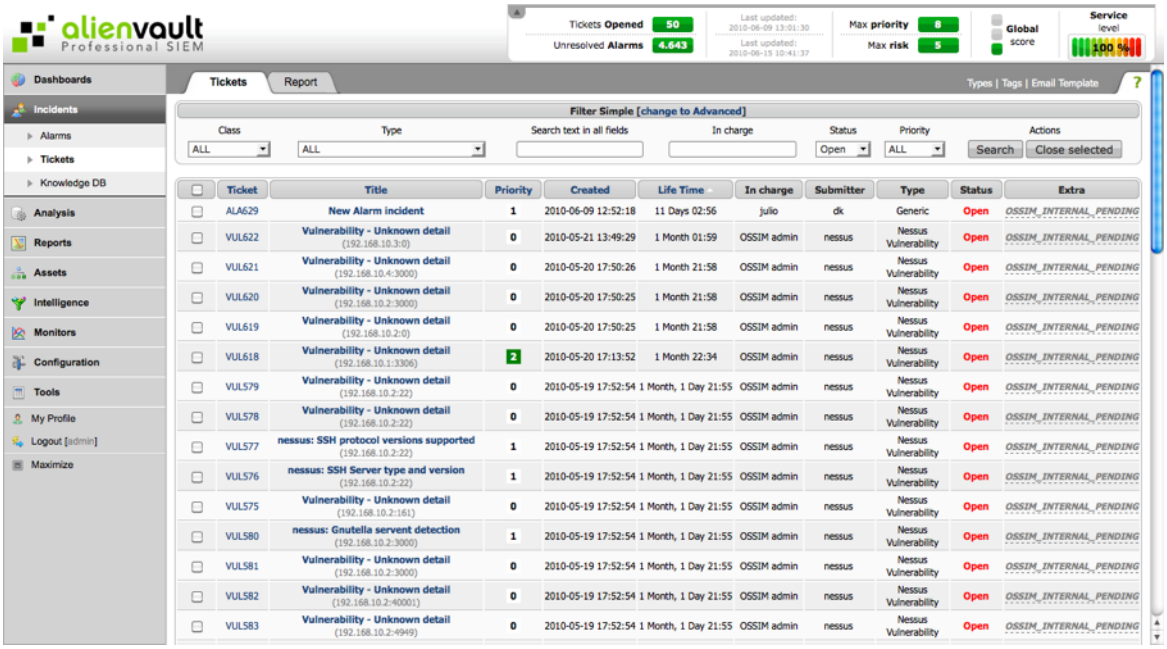
Tickets

Tickets

Incidents -> Tickets -> Tickets

Description

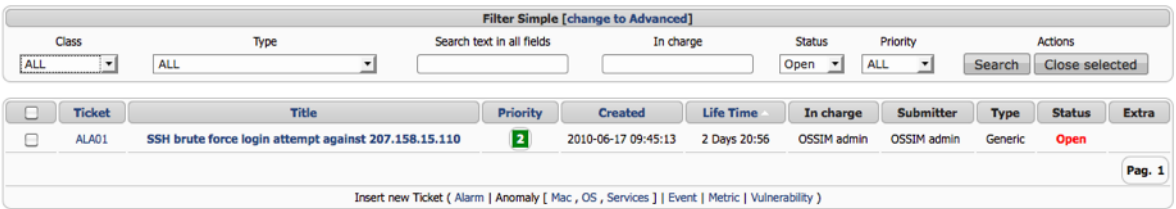
This is the ticketing system in AlienVault. This ticketing system allows users in AlienVault to work on the problems detected by using AlienVault. Tickets can be opened manually at any time, but also, some components in AlienVault can open tickets automatically, allowing users to work on the ticket.



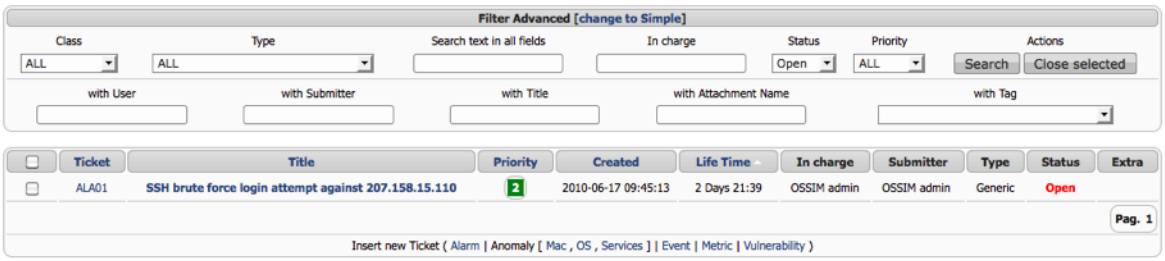
Usage

Filter

The simple filter allows you to quickly define a search criterion to return a set of tickets. You can filter based on ticket class (Alarm, Event, Metric, Anomaly or Vulnerability), ticket type, ticket status (open or closed) and ticket priority (0-10). The simple filter can also be used to search text in all fields in the ticket, and also filter based on the user in charge of the ticket.



In addition to the simple filter, the advanced filter will allow to filter based on users, submitters, title of the incident, attachment and tags, to access the advanced filter click on **change to Advanced**.



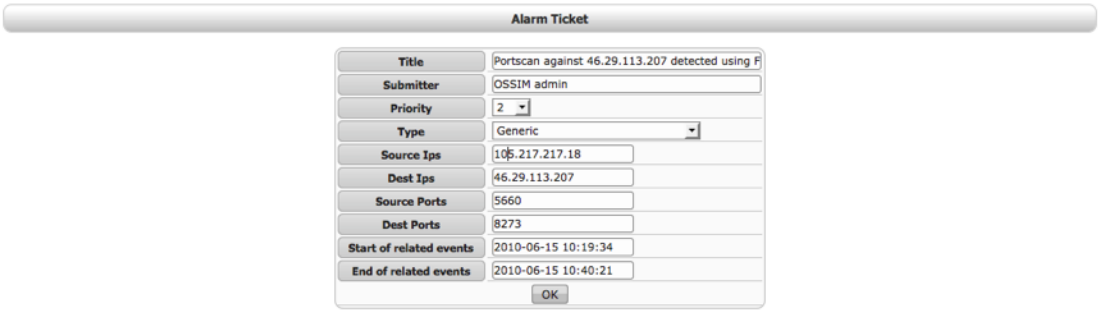
You can access more information about the ticket, or add to this information by:

- Clicking the ticket title
- Clicking the ticket number

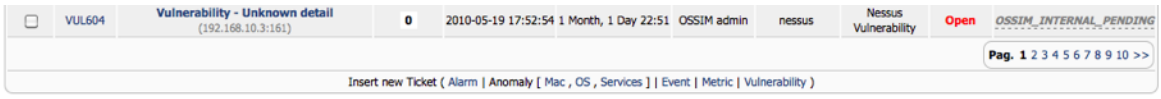
Manage Tickets

Open tickets

New tickets can be opened from the Alarm console (Incidents → Alarms), from the Risk Metrics panel (Dashboards → Risk (Risk Metrics)) and from the anomaly panel (Analysis → SIEM (Anomalies)). The information will automatically be added to the new ticket when accessed from these panels.



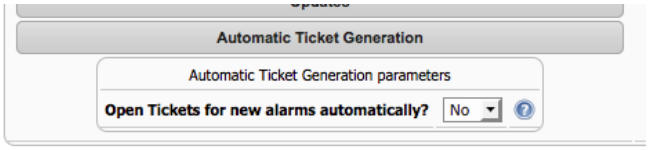
A new ticket can also be opened by clicking in one of the links in the bottom of the Ticketing system (Incident → Tickets):



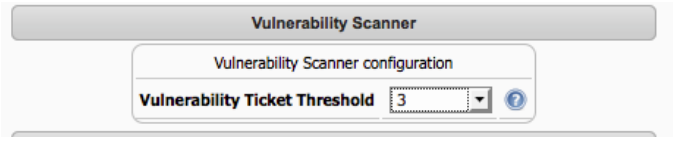
Open tickets automatically

Tickets can be opened automatically for alarms and vulnerability scanning results.

To open a ticket automatically when an alarm is generated go to Configuration → Main, expand the category **Automatic Ticket Generation** and set the parameter **Open Tickets for new alarms automatically?** to **Yes**.



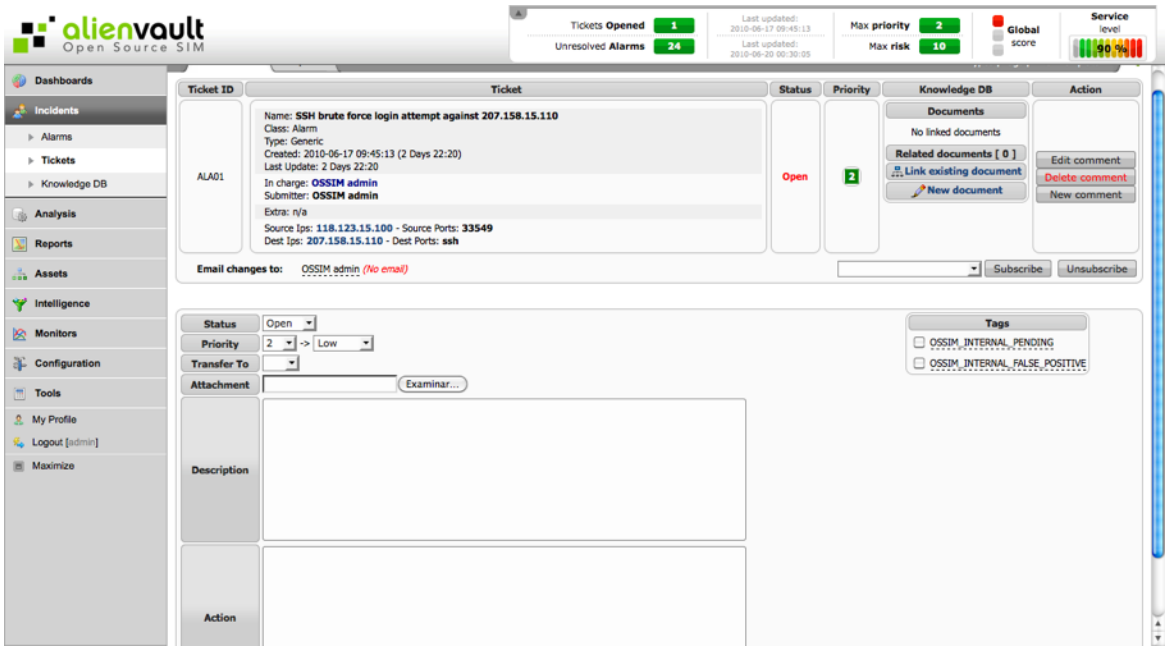
Tickets will be opened automatically whenever vulnerability is found in a host during the vulnerability scanning. You can configure the minimum risk vulnerability before a new ticket is opened. This configuration can be found in Configuration→ Main, within the category Vulnerability Scanner:



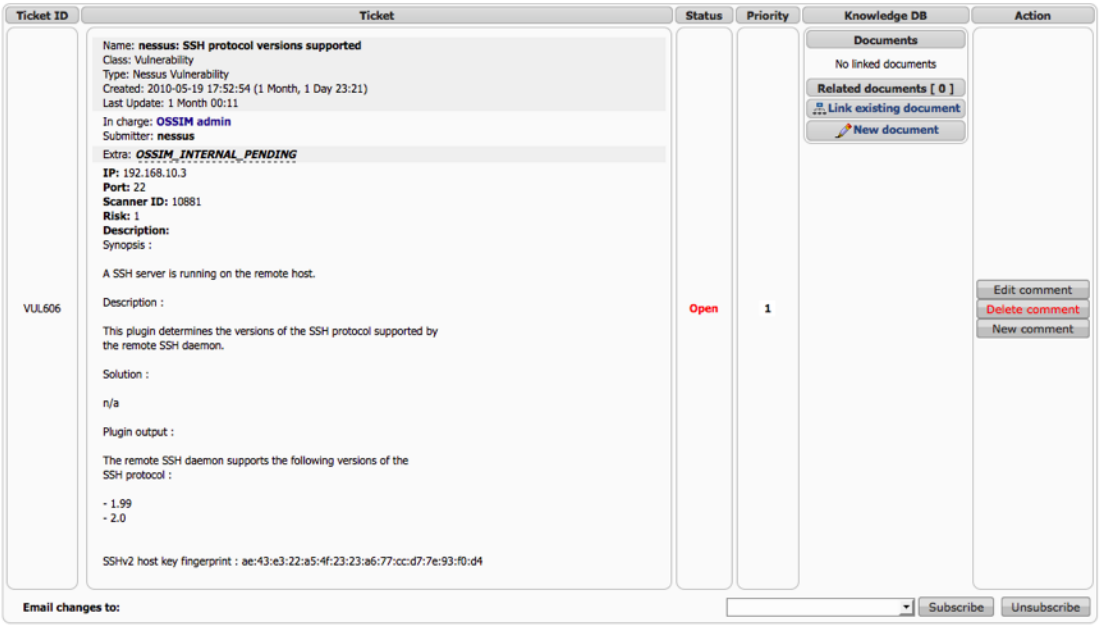
Setting this value too low will create a lot tickets in the system after a vulnerability scan, 3 or 4 will only open tickets for real vulnerabilities, not just for services identified in the hosts in our network.

Modify tickets

To do any modification in the ticket you will need to access the ticket information by clicking on the name of the ticket or in the ticket ID.



Once inside the ticket we want to modify we will find the following table in the top. This table will contain the original information that was included when creating the ticket as well as historical information of all the comments that have been added to this ticket.



This table will also show the status of the incident, the users that have been subscribed to this ticket, the actions that have been done to do a deeper analysis of the incident that originated this ticket and the list of documents that are linked to this ticket.

Comments

New comment

To include a new comment in a ticket click on the **New comment** button. A new comment has to be added to modify close or open the ticket, and to modify the priority of the ticket.

Edit comment

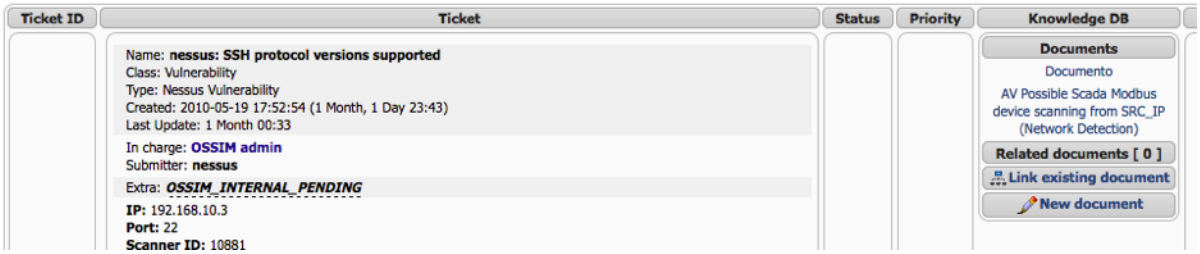
To edit a comment just click on the **Edit comment** button in the comment that you want to modify.

Delete comment

The admin user has special permissions allowing them to delete comments by clicking on **Delete comment** within the item that has to been selected.

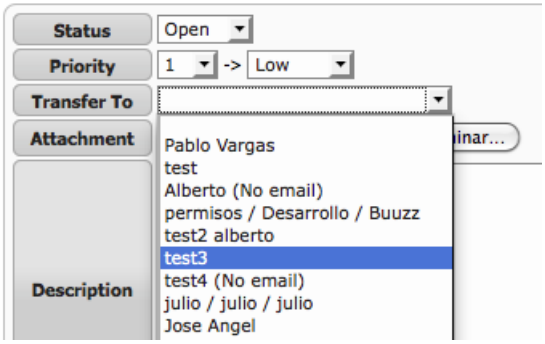
Knowledge DB

Documents from the Knowledge DB can be linked to a ticket. This allows linking, for example, a document explaining how to remove a known trojan, a network map, or a list of people that should be contacted whenever there is a problem in one of the networks.



Transfer to another user

A user will be in charge of every ticket, when a new ticket is created the user that created the ticket will be in charge of it. The ticket can be transferred to another user using the following form when including a new comment in the ticket:



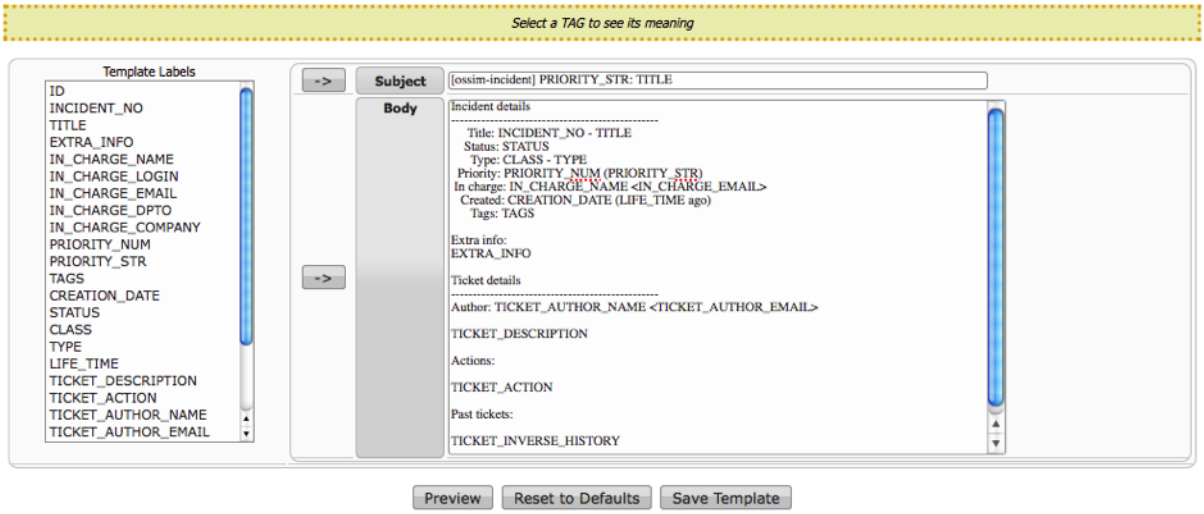
Attach a file

Files can be attached to the ticket when including a new comment in the ticket.

Subscribe Users to a ticket

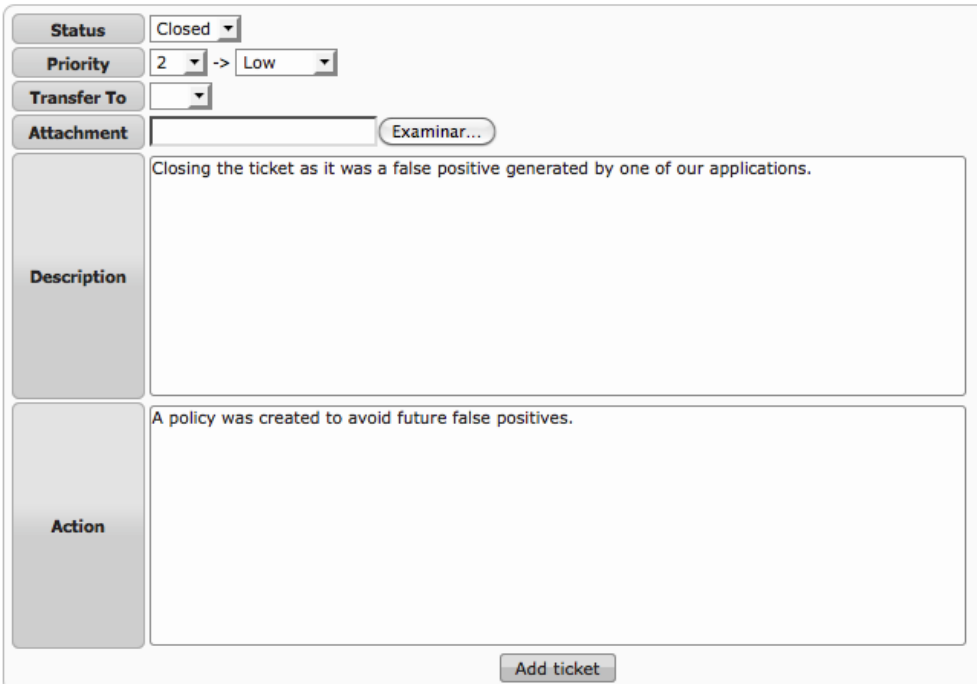
Users defined in the AlienVault Web Interface can be subscribed to a ticket so they can receive an e-mail whenever something is changed in the ticket they are subscribed to. To do this just select the user you want to subscribe to the ticket and click on **Subscribe**. To unsubscribe a user of a ticket click on the **Unsubscribe** button.

You can modify the format of the e-mail that will be sent to users subscribed to an incident by clicking on **E-mail template** in the upper right corner. When defining the e-mail template you can use specific keywords or tags that can be replaced by the value of the variable whenever the e-mail is being sent.



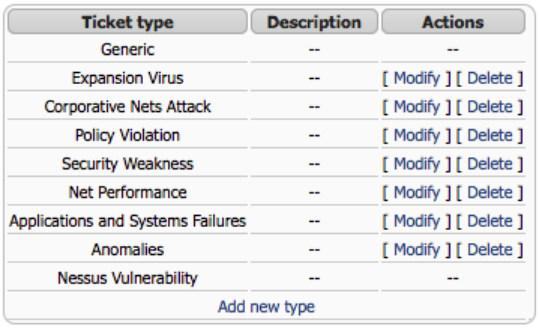
Close tickets

In order to close or re-open a ticket you will have to include a new comment, modify the status, and explain in the description field why the ticket was closed or reopened.



Types

To classify the tickets in the system you can use “types”. Some types come defined by default but you can define your owns by clicking on **Types** in the upper right corner of the interface.



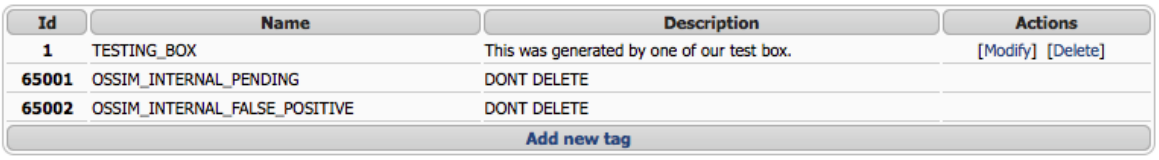
Ticket type	Description	Actions
Generic	--	--
Expansion Virus	--	[Modify] [Delete]
Corporative Nets Attack	--	[Modify] [Delete]
Policy Violation	--	[Modify] [Delete]
Security Weakness	--	[Modify] [Delete]
Net Performance	--	[Modify] [Delete]
Applications and Systems Failures	--	[Modify] [Delete]
Anomalies	--	[Modify] [Delete]
Nessus Vulnerability	--	--
Add new type		

Tags

Tags can be used to quickly append information. Two of the tags come by default; they are used in tickets opened by the vulnerability scanning:

- **AlienVault_INTERNAL_PENDING**: If this tag is set, the vulnerability scanner will not open the same ticket again.
- **AlienVault_FALSE_POSITIVE**: If this tag is set, the vulnerability will be marked as a false positive and it will not be opened again during a future scan.

You can add new tags by clicking on **Tags** in the upper right corner.



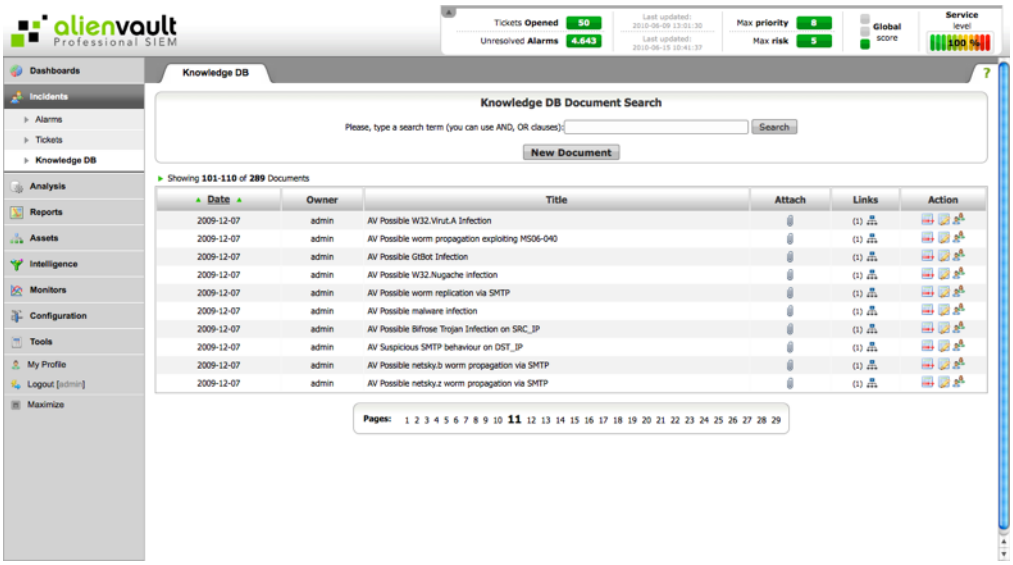
Id	Name	Description	Actions
1	TESTING_BOX	This was generated by one of our test box.	[Modify] [Delete]
65001	OSSIM_INTERNAL_PENDING	DONT DELETE	
65002	OSSIM_INTERNAL_FALSE_POSITIVE	DONT DELETE	
Add new tag			

Knowledge DB

Incidents -> Knowledge DB

Description

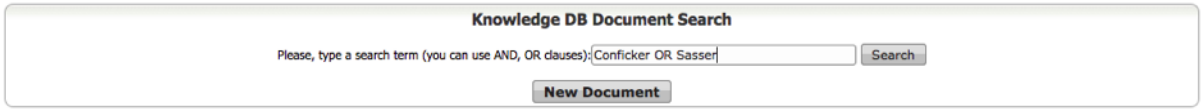
As the name indicates, the Knowledge DB tab provides access to a user-defined, searchable knowledge base of solutions to incidents. New documents can be created with a title, description, and key words that may be linked to a host, a host group, a network, a network group, a ticket, a directive or a type of event. One or more files may be attached to each document.



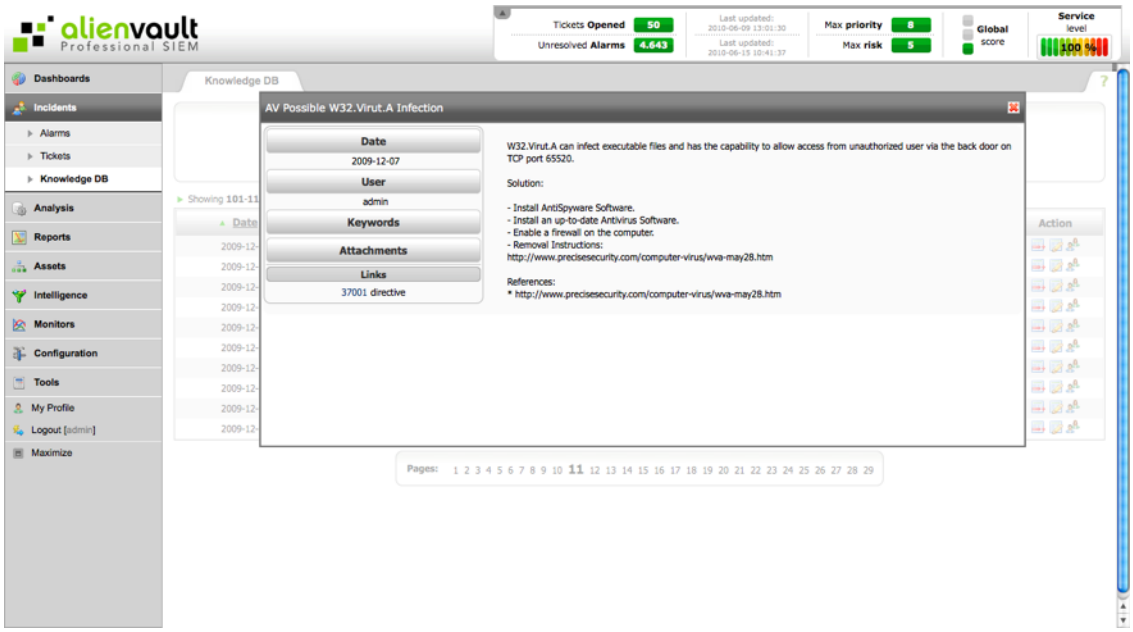
Usage

View Documents

The upper form can be used to search through documents, it is possible to search for a document using AND and OR operators.

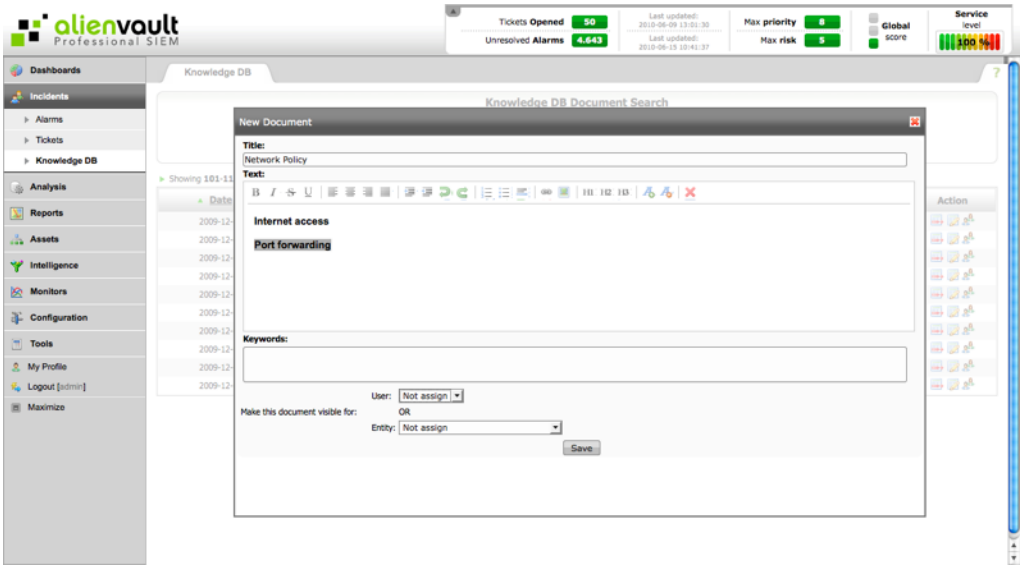


To access a document click on the name of the document:

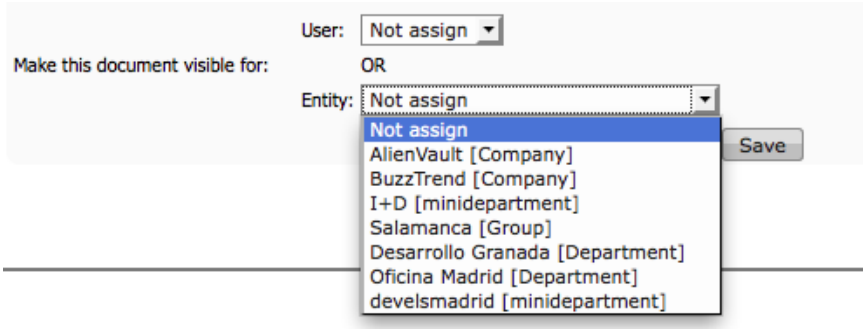


New Document

A new document can be added to the Knowledge Database by clicking on **New Document**. The system provides a rich text editor to format the text and offers the possibility of including images in the documents.



Each document can be visible for a user or for an entity:



Edit Document

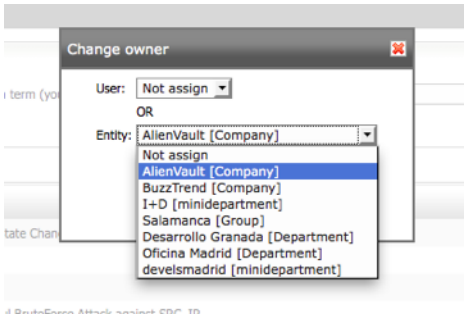
To edit a document click on this icon  next to the name of the document that you wish to edit.

Delete Document

To delete a document click on this icon  next to the name of the document that you wish to delete.

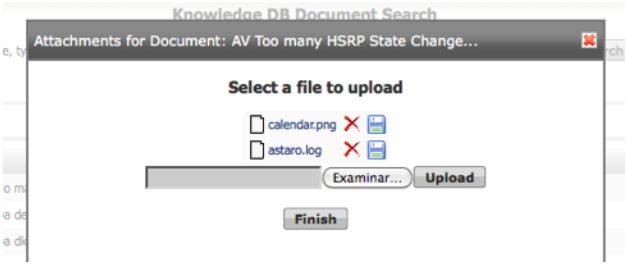
Change Owner

To change the owner of the document click on the icon  next to the document that will modify its ownership.



Attach files

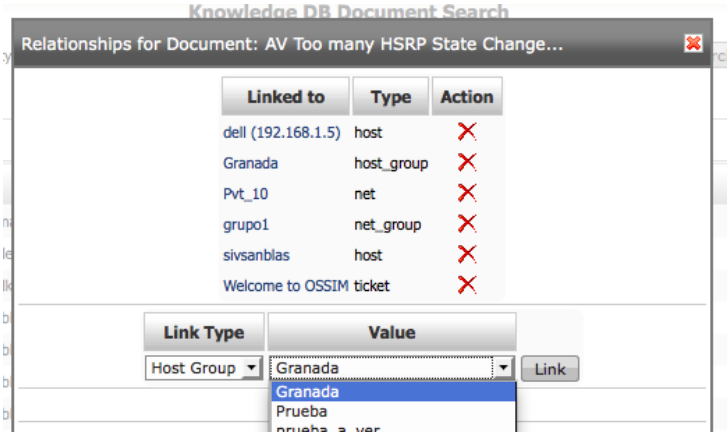
To attach a file to a document in the Knowledge DB click on the icon  next to the name of the document.



Link Documents

A document in the Knowledge DB can be linked to a host, a host group, a network, a network group, a ticket, a directive or a type of event.

To link a document just click on the icon  . You will get the following form that will allow to link and unlink the document with the different objects in your inventory, and with tickets, directives and events:



Analysis

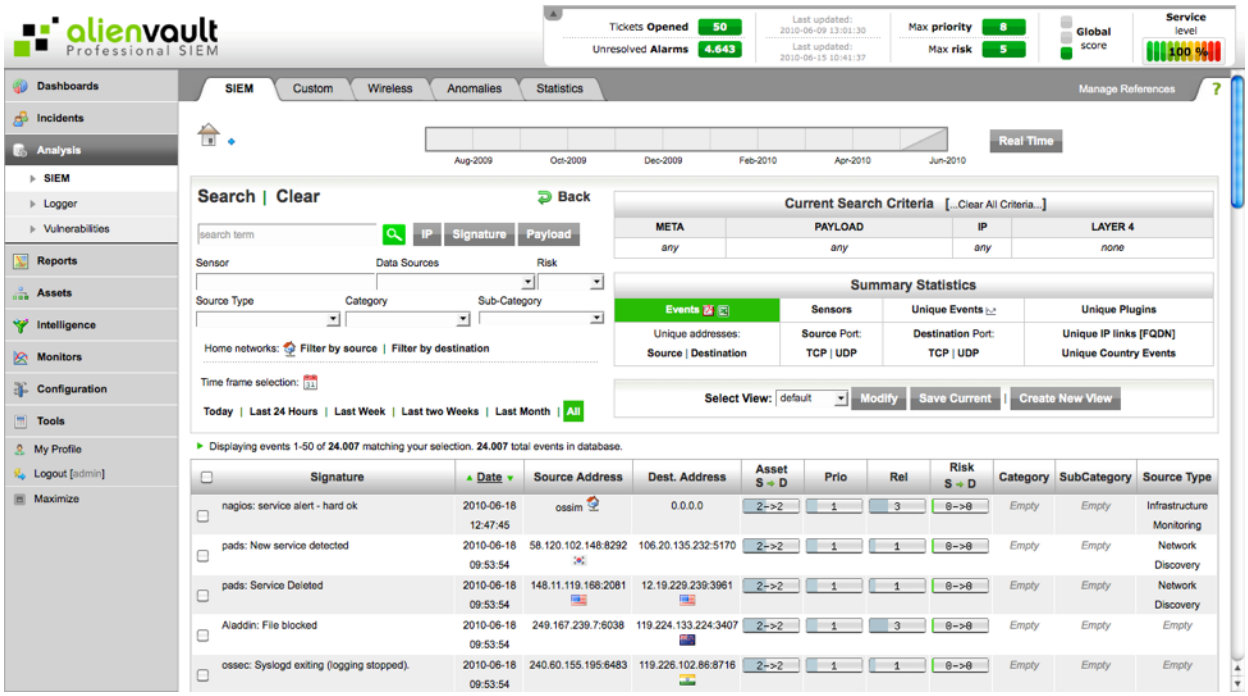
SIEM

SIEM

Analysis -> SIEM -> SIEM

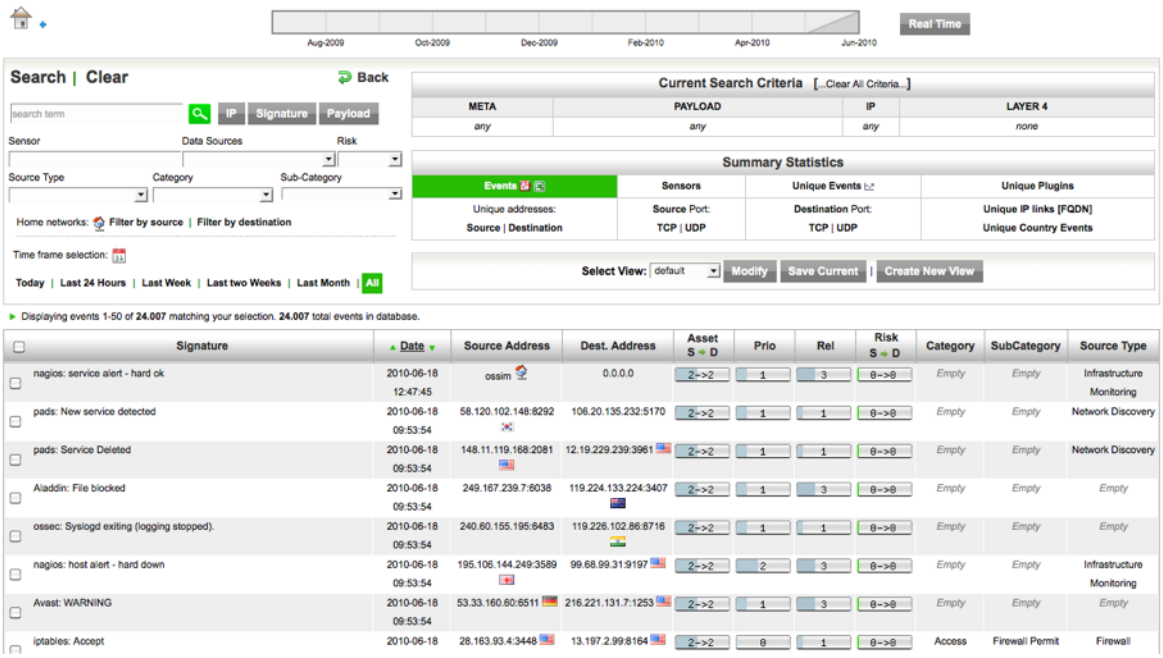
Description

The SIEM tab gives access to all the events stored (SQL Storage) when using the SIEM functionality of AlienVault. It allows the user to do a forensic analysis of all events that been processed by the AlienVault SIEM.



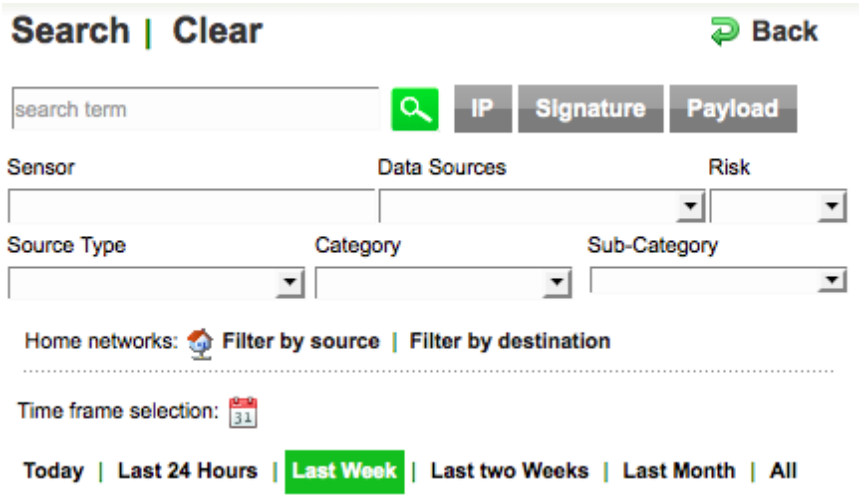
In the SIEM profile, events are qualified (A risk is calculated for every event) and correlated. Correlation generates new events that will also be stored in the SQL database. Alarms are a special type of event, with a risk higher than 1, but, as events, they will also be stored in the SIEM profile, and you will be able to see them in both Incidents → Alarms, but also in Analysis →SIEM.

The SIEM forensic console is divided into different sections that will be explained in different sections:

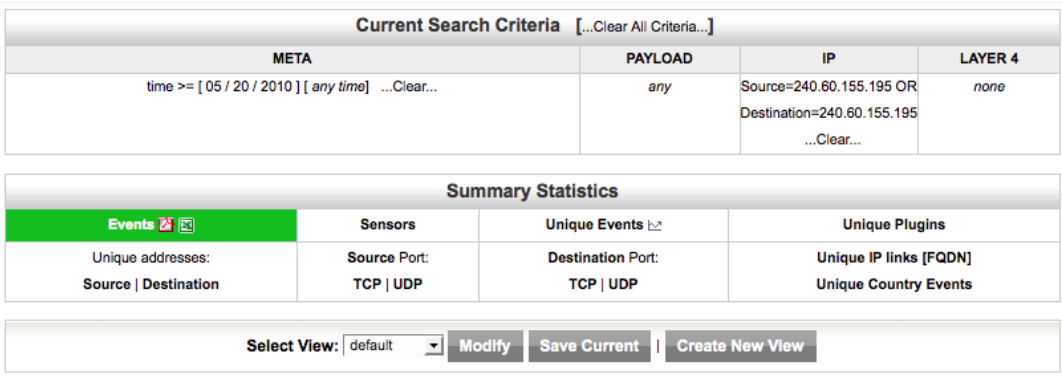


In the top of the screen we will find a trend graph showing the number of events in a time line. This time range will be modified based on the current time search criteria. On the left we have a link to see events arriving to the AlienVault Server in Real Time:

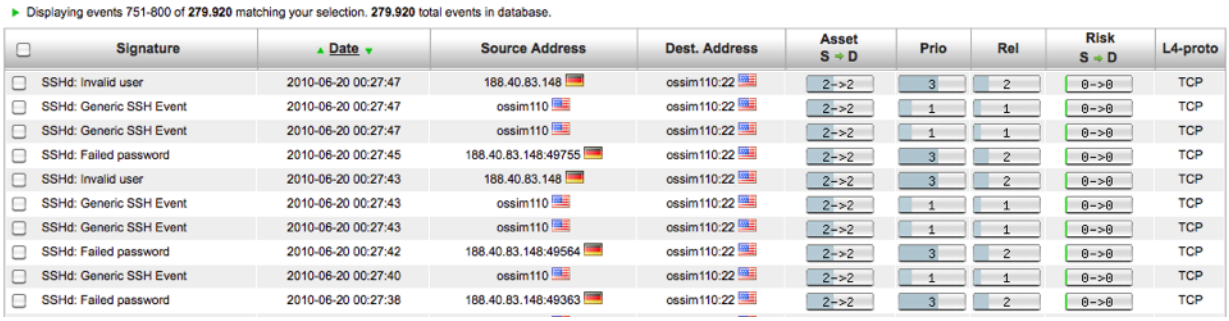
IIn the upper left corner you will find two links, the first one, **Search** links to the advanced search, the second one, **Clear** will clear all search criteria. In this block you can also find search boxes and drop boxes that will help you searching certain events. At the bottom of this block, different links allow you to set the time and range of the events that will be used when doing the forensic analysis.



In the upper right side of the screen, we can find the current search criteria that are being applied when getting events from the SQL database. We can also find access to summary statistics that will show statistics based on the search criteria that is currently being used. On the bottom of this block you will be able to configure a custom view to see certain fields of the events stored in the SQL database.



The list of events is shown in the bottom of the screen.

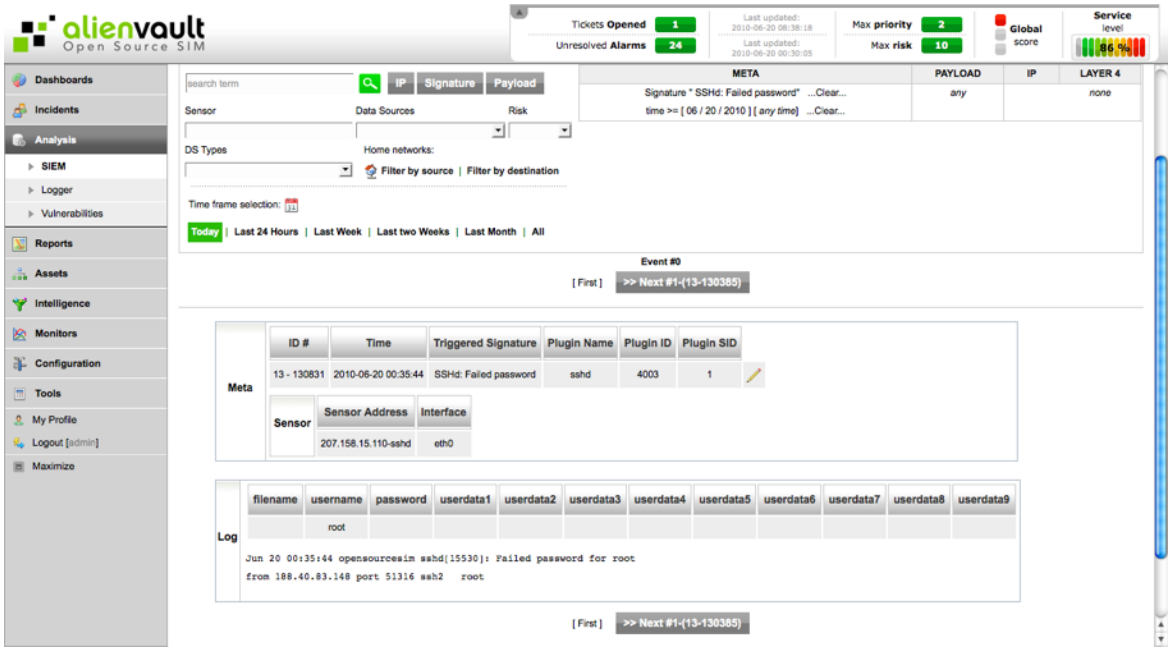


The list of fields showed can be customized, by default the following fields will be visible for every event:

- **Signature**: A brief description of the event.
- **Timestamp**: This indicates the date and time when the event occurred.
- **Source Address**: This is the address of the source host, that can be the name of the host, its IP, or its IP and port.
- **Dest. Address**: This is the address of the destination host that can be the name of the host, its IP or its IP and Port.
- **Asset S→D**: Asset Value of the Source host of the event (S) and Asset Value of the destination host in the event. The Asset value is a number between zero and five.
- **Prio**: This is the priority of the event.
- **Rel**: This is the reliability of the event.
- **Risk S→D**: Risk calculated based on the source of the event (S) and risk calculated based on the destination of the event (D).

Event Information

The SIEM stores the original event that was collected by one of the collectors deployed in the monitored network, or, in case of Snort events, the network payload that has generated a snort alert.



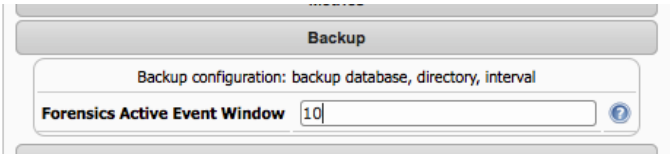
The system provides some utilities to work with the payloads (Shellcode Analysis, Download in Pcap format…).

Events in Database

Depending on the hardware and on the number of events per second that you are getting you may be able to store in the SQL Database a certain number of events. When storing a lot of events in the SQL Database, the analysis gets slower and it is harder to navigate through the AlienVault Web interface.

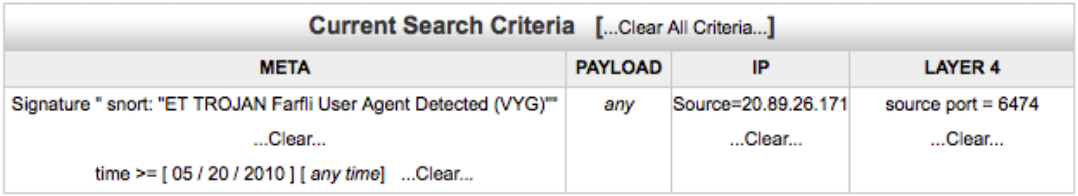
For this reason events are rotated every few days, in a company that is only generating a few events per day you will be able to store events of for many years, but if a company is generating a huge number of events and your hardware can not deal with that amount of events you may need to rotate events every 3 days.

By default the system will only keep in database the events of the last 5 days, but this can be configured modifying the parameter **Forensics Active Event Window** in Configuration → Main (Backup).



Active filters

When navigating through the SIEM console new filters can be applied, reducing the number of events you are working with. It is very important to be aware of the current search criteria, because you may reach the point in which all events have been filtered due to your search criteria.

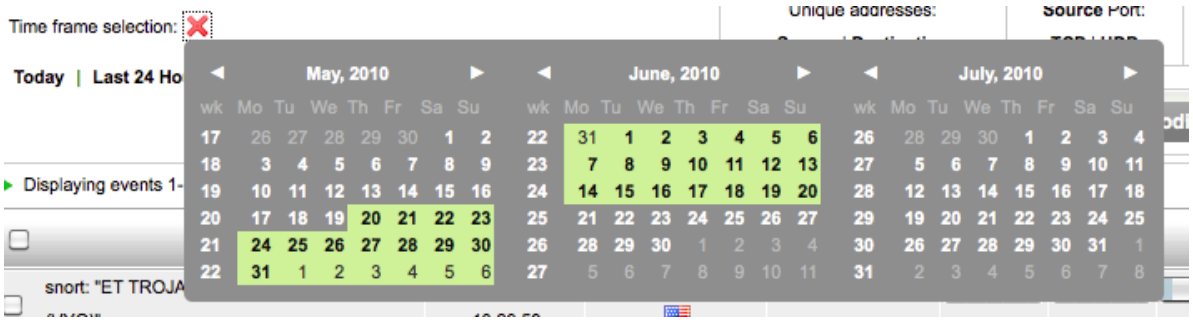


Usage

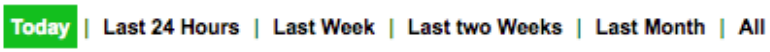
Time range

When selecting the time range you want to work with you can reduce the amount of events you are working with and the analysis will be much faster.

It is possible to select the time frame using a calendar displayed when clicking on the icon  :



Or using one of the predefined time ranges:



The time range will appear as a filter in the Search Criteria box.

More precise time frame definition can be set using the Advanced Search functionality.

Clickable columns

When working with a list of events or in any summary statistics view, it is possible to click in the name of the column to order the information based on the column that has been clicked, clicking again in the same column will show the information in reverse order.

Simple Search

The Simple search allows the user filtering events by name of the event (Signature), by an IP address (Source or Destination), or by text contained in the original event that was collected by AlienVault (Payload).

Logical operators AND/OR can be used (In capital letters) when searching events by Signature or by IP address:

When searching new filters will be applied and shown in the **Search criteria** box. You can click only one filter clicking on **Clear** next to the filter you wish to clear.

Current Search Criteria [...Clear All Criteria...]			
META	**PAYLOAD**	**IP**	**LAYER 4**
any	*any*	Src or Dest=192.168.0.2 OR Src or Dest=192.168.2.2 ...Clear...	*none*

Summary Statistics

Summary statistics provides useful information (Data is retrieved from the database using the search criteria) grouping events using different criteria:

- **Sensors**: Events grouped by sensor
- **Unique Events**: Events grouped by type of event
- **Unique Plugins**: Events grouped by plugin (Detector)
- **Unique addresses**: Events grouped by source/destination
- **Source/Destination Port**: Events grouped by port
- **Unique country Events**: Events grouped by country

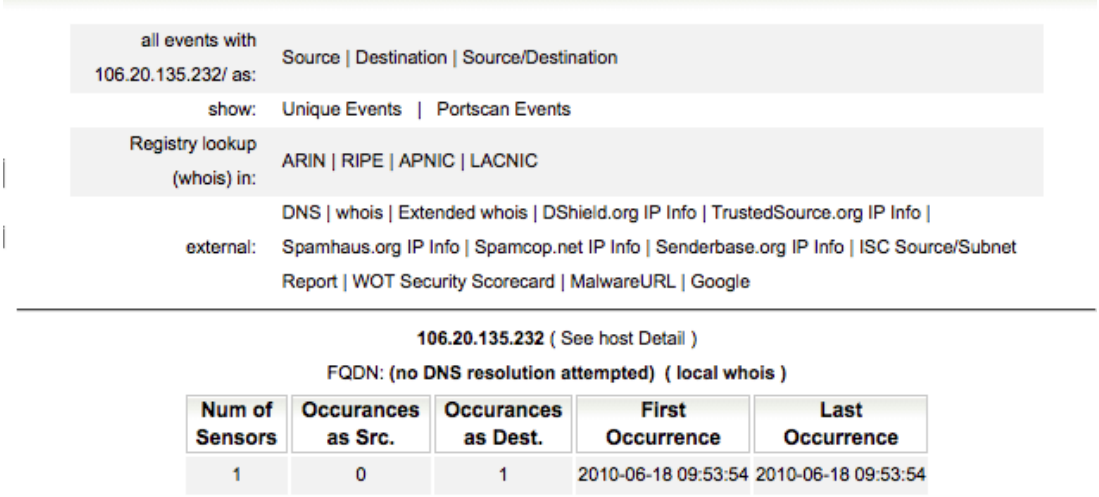
When using these summary statistics you will be able to click on some of the values. This may apply new search criteria.

Signature	Total #	Sensor #	Src. Addr.	Dst. Addr.	First	Last
Aladdin: File blocked	1462 (6%)	6	1462	1462	2010-06-08 17:06:22	2010-06-18 09:53:54
Avast: WARNING	1447 (6%)	6	1447	1447	2010-06-08 17:06:04	2010-06-18 09:53:54
directive_event: Prueba directiva	794 (3%)	3	794	794	2010-06-15 10:12:44	2010-06-16 10:40:24
gfi: Deleted	766 (3%)	6	766	766	2010-06-08 17:20:12	2010-06-18 09:53:52
gfi: Quarantined	713 (3%)	7	713	713	2010-06-08 17:06:16	2010-06-18 09:53:44

All the information displayed can be exported as a PDF file or as a CSV file, the information will be exported as it is been shown in the Web interface, keeping always the different search criteria. To do this just click on the icon (PDF) or (csv) next to the enabled view.

IP information

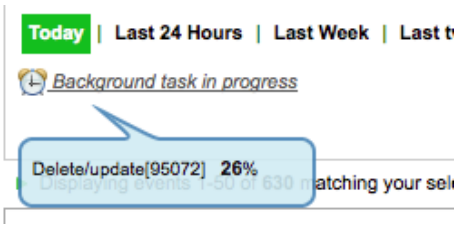
When clicking on an IP address you will have easy access to all the information stored by the system regarding that IP address. The system also provides links to external websites that offer interesting information (DNS, Spam black lists, Malware information…) in reference to public IP addresses.



Delete events

To delete an event you need to mark the checkbox next to the name of the event and in the bottom click on **Delete event**. To delete all events on screen click on **Delete ALL on Screen**. To delete all events matching the search criteria click on **Delete entire query**.

Deleting events is a heavy task that may take a while, be patient and do not close the browser until all events have been deleted.



Wireless

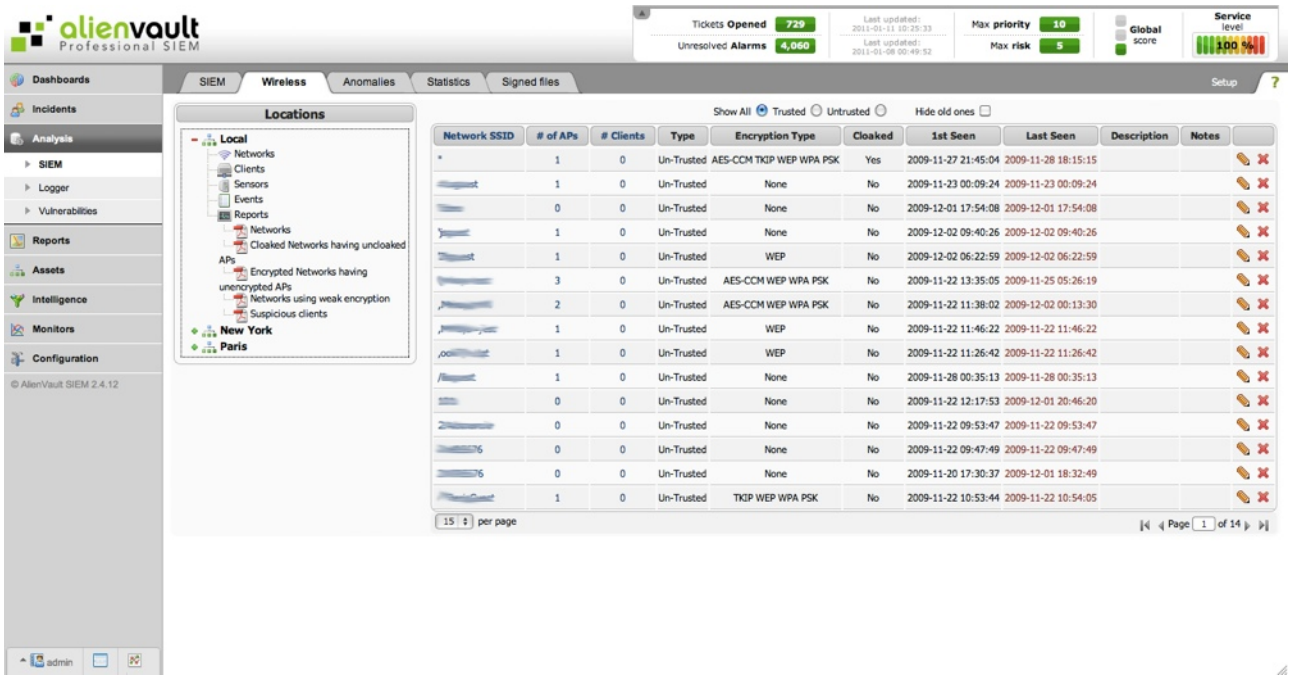
Analysis -> SIEM -> Wireless

Description

Organizations that require Payment Card Industry's Data Security Standard (PCI DSS) compliance need to follow a set of procedures when deploying 802.11 Wireless Local Area Networks (WLAN). AlienVault includes a Wireless Compliance module that helps organizations that require PCI DSS compliance.

This module was developed using the information provided by Kismet, an Open Source wireless network detector, sniffer, and intrusion detection system.

The PCI DSS module includes reports and statistics needed to perform a PCI DSS audit successfully. To run this module you must have kismet working in wireless sensors that feed the system with information about wireless networks in the environment that it is being monitored.



Locations

Places of activity of the corporation that need to be monitored. Each location can have one or more wireless sensors. By configuring the various locations you can filter by location when generating reports.

Wireless Sensors

The wireless sensor should be with Kismet configured to send information to AlienVault in .xml format. AlienVault processes this information to fill in the tables that are used to generate the reports.

Usage

Reports

The information regarding the wireless compliance monitoring is displayed in a screen divided in two parts. The left side shows the available locations, to show the information of each location click on icon next to the name of the location. Information is displayed in the right side.

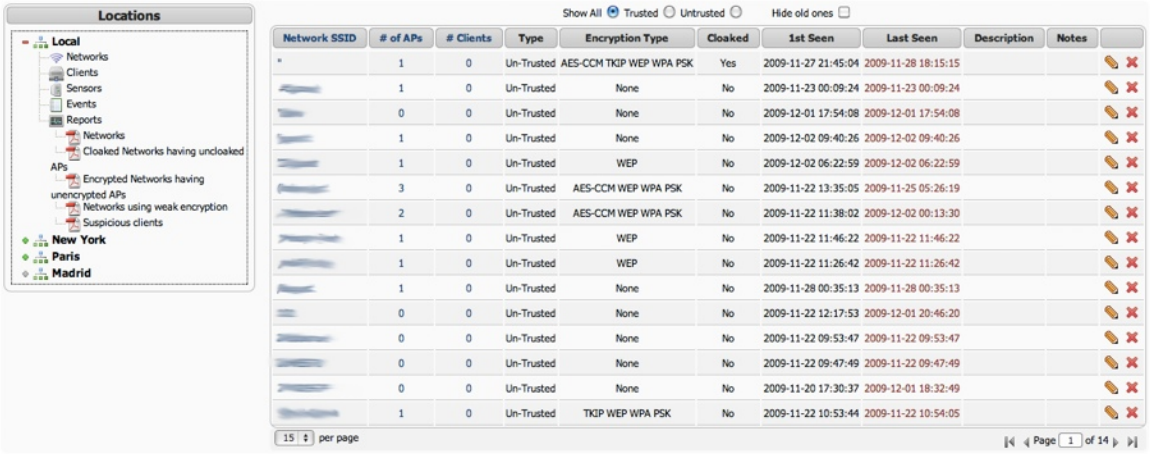
Within the branch of each location, all available reports and statistics are displayed. The following reports can be accessed within this menu:

- Networks
- Clients
- Sensors
- Events
- Reports
  - Networks
  - Cloaked networks having uncloaked APs
  - Encrypted Networks having unencrypted APs
  - Networks using weak encryption
  - Suspicious clientsNetworks

Networks

This report shows a list of wireless networks that can be found in the location. Each network is displayed with the following properties:

- **Network SSID**: Network Service Set IDentifier
- **# of APs**: Number of Access Points within this Wireless Network
- **# of Clients**: Number of clients connected to this Wireless Network
- **Type**: Trusted network or Un-trusted network
- **Encryption** Type: Type of encryption used within the wireless network (AES-CCM, TKIP, WEP, WPA, PSK...)
- **Cloaked**: Wether the wireless network is invisible or not
- **1st Seen**: When was the wireless network first seen
- **Last Seen**: When was the wireless network last seen
- **Description**: Description of the wireless network
- **Notes**: Optional field to enter information manually regarding this wireless network



Networks displayed can be filtered using the form on top of the table displaying the wireless networks to show only trusted or un-trusted networks and also hiding the old networks.

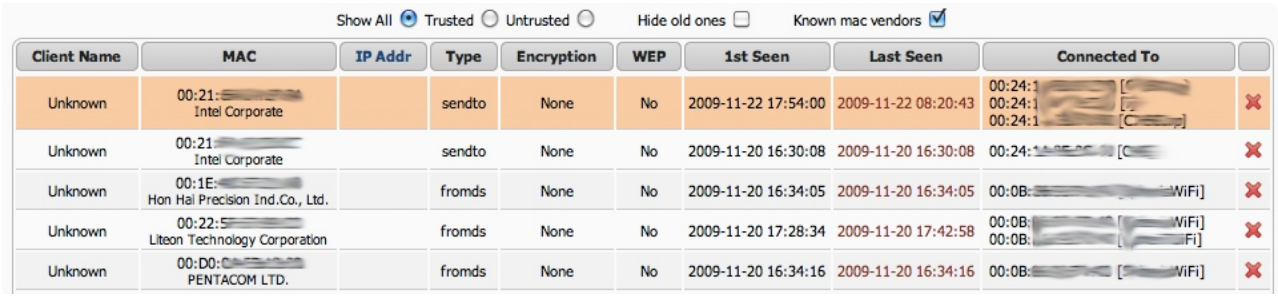
Wether the network is trusted or not can be modified manually by clicking on the symbol  in the line representing the wireless network. Clicking on that icon will show the following form that can also be used to enter notes and a short description about the wireless network.

To delete a wireless network from the list click on  in the line representing the Wireless Network.

Clients

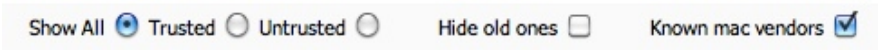
This report shows a list of clients connected to the wireless networks. Each client is displayed with the following properties:

- **Client Name**: Name of the wireless client
- **MAC**: Physical address of the network device used by the client to connect to the wireless network (Mac address)
- **IP Addr**: IP address used within the wireless network by the client
- **Type**: Network Connection Type: Infrastructure, Ad-Hoc, tods, sendto, fromds, interds
- **Encryption**: Encryption type: WEP, WPA... Weak
- **WEP**: WEP encryption (Yes or Not)
- **1st Seen**: When was the client first seen
- **Last Seen**: When was the wireless network last seen
- **Connected to**: List of wireless network the client is connected to



To delete one of the clients in the the list click on  in the line representing the client that you wish to delete.

Clients displayed can be filtered using the form on top of the table displaying the wireless networks to show only trusted or un-trusted clients and also hiding the old clients.



The **Known mac vendors** checkbox will enable or disable displaying the network card vendor next to the mac address of the client.

Sensors

This report shows the Wireless Sensors monitoring the location. It displays also the status of the sensor (Enabled or Disabled).

By clicking on  you can modify the properties of the Wireless Sensor.

Events

This report shows Kismet events collected in each location grouped by type of event.

Reports (Networks)

By clicking on **Networks** within the reports branch, a report in .PDF format will be generated containing a list of networks that can be accessed in each location.

Reports (Cloaked networks having uncloaked APs)

By clicking on **Cloaked networks having uncloaked APs** within the Reports branch a report in PDF format will be generating containing a list of the cloaked networks that have uncloaked Access Points.

Reports (Encrypted Networks having unencrypted APs)

By clicking on **Encrypted Networks having unencrypted Aps**, within the Reports branch, a report in .PDF format will be generated containing a list of the encrypted networks that have unencrypted Access Points giving access to that wireless network.

Reports (Networks using weak encryption)

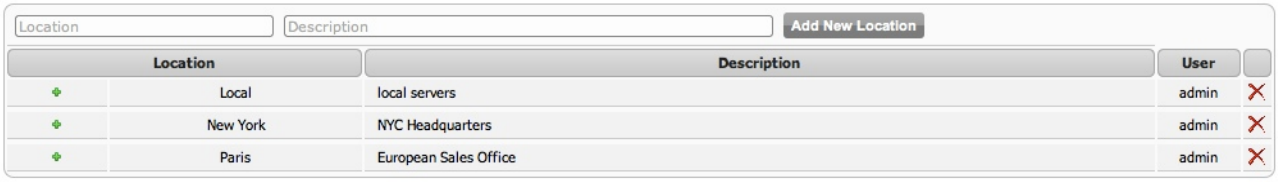
By clicking on **Networks using weak encryption** within the Reports branch a report in PDF format will be generating containing a list of networks using weak encryption (No encryption, WEP...).

Reports (Suspicious clients)

By clicking on **Suspicious clients** within the Reports branch, a report in .PDF format will be generated containing a list of clients that have suspicious behavior.

Setup Locations

The different locations of the corporation are configured by clicking in **Setup locations** in the upper right.



New Location

To insert a new location enter the name of the location and the description and click on **Add New Location**. After adding the location click on  next to the name of the location to add the Wireless sensors that are monitoring that location.

Select the sensor from the drop menu and enter the optional properties for that sensor:

- **Model**: Model of the wireless device used within the wireless sensor.
- **Serial**: Serial number of the wireless device that it is being used to monitor the wireless network
- **Mounting Location**: Description of the place where the sensor has been deployed.

To delete a sensor from a location click on the symbol  next to the sensor that you wish to delete.

Modify Location

To modify the properties and the sensors related to a location click on  next to the name of the location that you want to modify.

Delete Location

To delete a location click on  next to the location that you wish to delete.

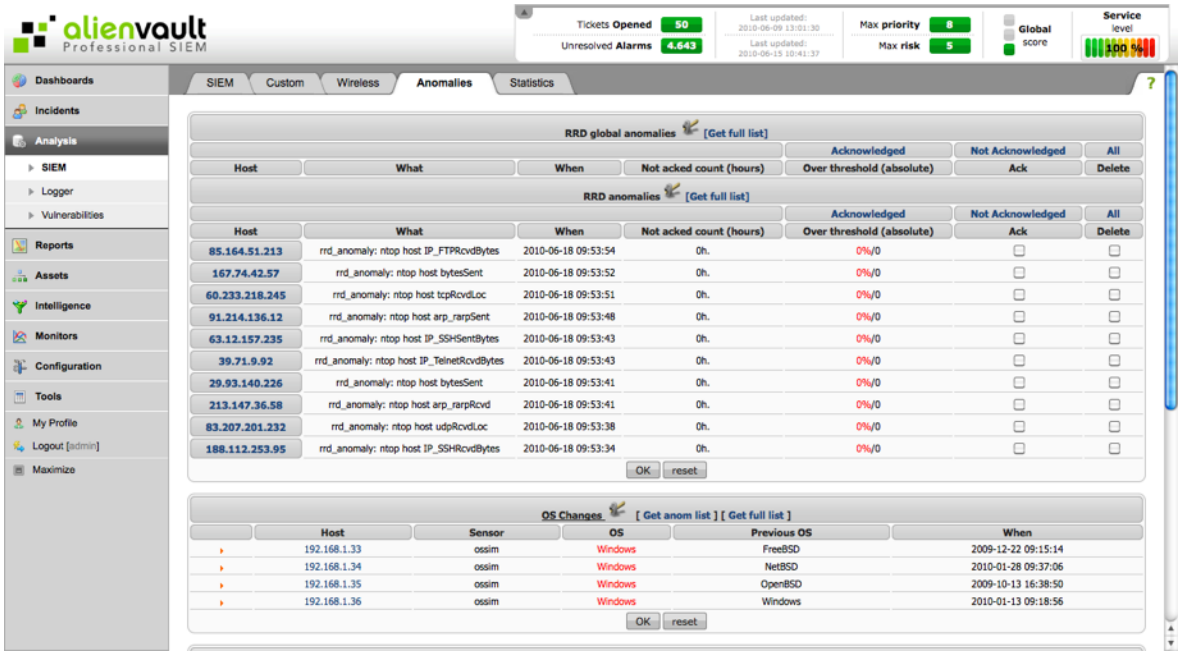
Anomalies

Analysis -> SIEM -> Anomalies

Description

The anomalies tab shows five types of anomalies:

- RRD global anomalies. (Ntop & RRDplugin)
- RRD anomalies. (Ntop & RRDplugin)
- Operating system changes. (P0f)
- Mac Address changes. (Arpwatch)
- Service version changes.(Pads)



From this tab you can acknowledge these changes, ignore them and generate related tickets.

Usage

Click on the orange triangle next to the anomaly to see all changes that have happened in the anomaly.

An anomaly will be generated whenever an event is giving different information than the one that the AlienVault inventory has.

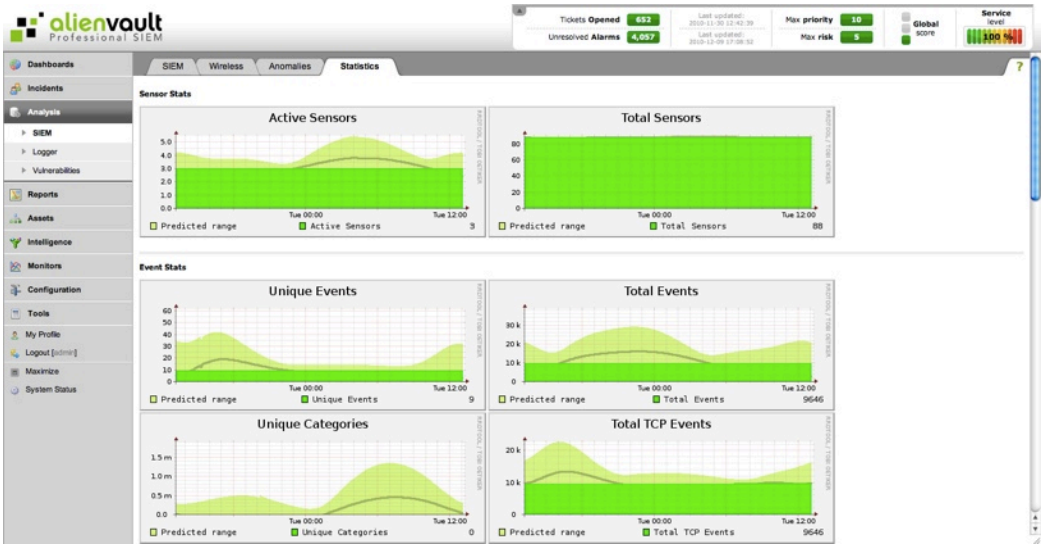
Statistics

Analysis -> SIEM -> Statistics

Description

The Event Stats page shows event statistics in a graphical format related to:

- Sensor
- Event
- IP addresses
- Ports



Usage

This stats may cause performance problems due to the heavy queries that have to be done in the SQL Database every often. For this reason these statistics are not enabled by default.

To enable this functionality go to Configuration → Main (Advanced), expand the category AlienVault **Framework Daemon** and set the variable **Enable EvenStats** to Enabled

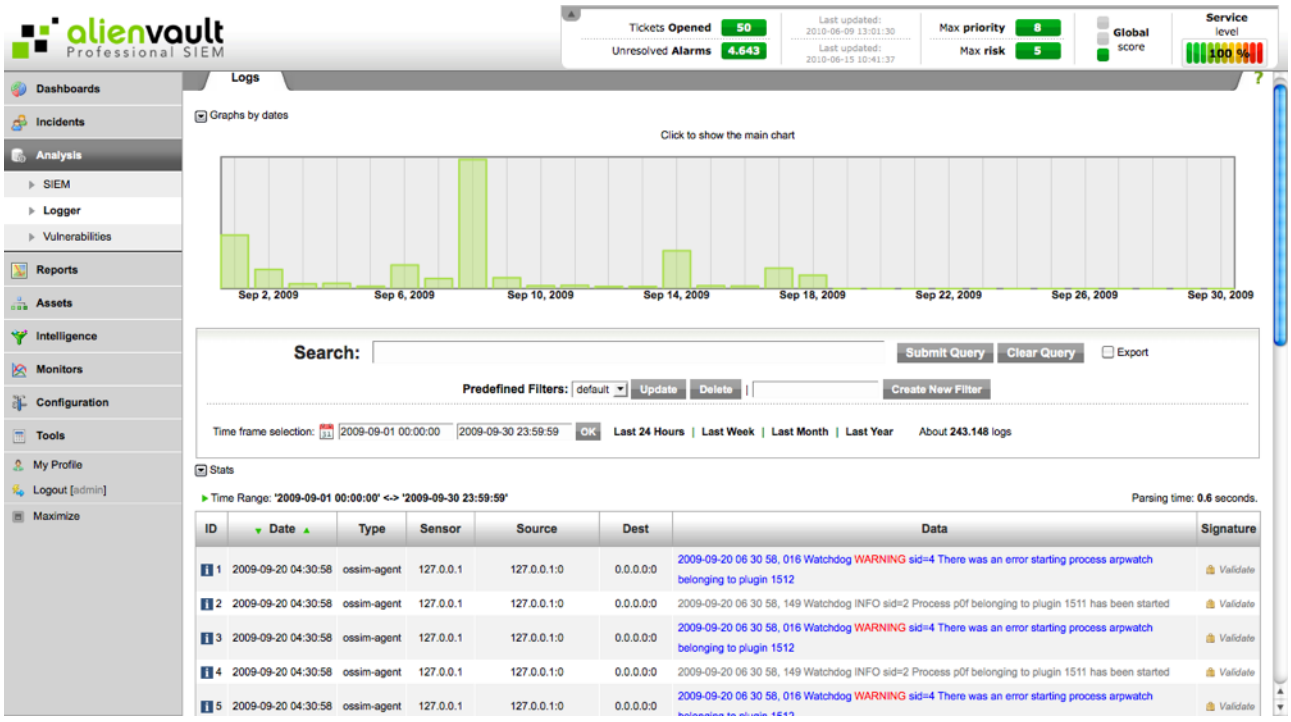
Logger

Logger

Analysis -> Logger -> Logs

Description

The Logger allows for storage of large volumes of data while ensuring its admissibility as evidence in a court of law. The Logger provides an additional database specifically geared for massive, long-term, forensic archiving. The Logger collects data in its native format, digitally signs, and time-stamps the data. The data is then securely stored preserving data integrity; whereas the SIEM database is designed for the rapid and versatile analysis required for attack detection and response.



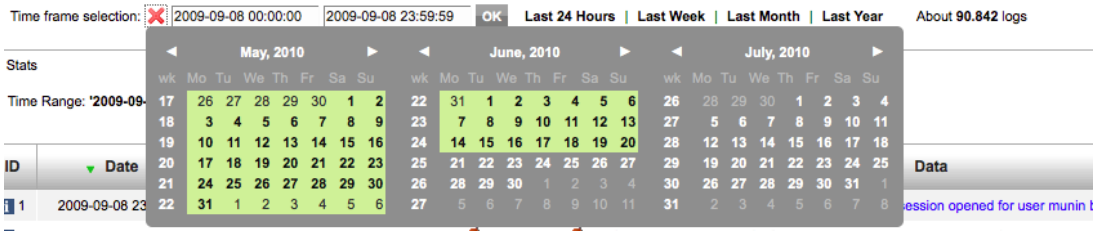
In the Logger, events are stored in the file system, using an AlienVault specific schema of directories and files

Usage

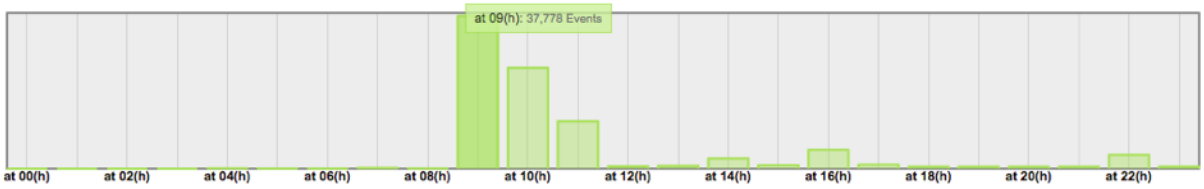
Time range

The logger analysis requires working with a huge amount of data. If you reduce the amount of events you are working with the analysis will be much faster.

You can select the time range you want to work with using a calendar or using one of the predefined time ranges.



Clicking on the bars of the graph on the top will also update the time range.

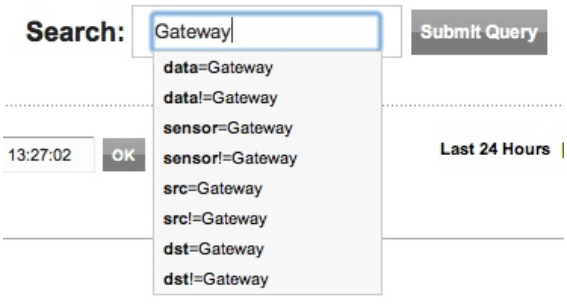


Search

The search for events stored in the Logger implements auto-completion based on the text that you type. For example, if you enter a host name, the system will suggest searching for the defined value in the host field of the events.

The following syntax can be used when searching over the events in the Logger:

- **sensor:** Ip address or name of the AlienVault Sensor that collected the event. Eg: sensor=Vegas sensor=172.2.2.1
- **src**: Source of the event in IPV4 format or name of the host used in the AlienVault inventory. Eg: src=192.168.2.1 src=Web_2000
- **dst:** Destination of the event in IPV4 format or name of the host used in the AlienVault inventory. Eg: dst=192.168.1.1 dst=gateway
- **plugin**: Name of the plugin (Data Source connector). Eg: plugin=snort
- **plugingroup**: Name of the plugin group. Eg: sourcetype=Facebook_events
- **src_port**: Source Port. Eg: src_port=34000
- **dst_port**: Destination Port. Eg: dst_port=80
- **sourcetype**: Filter by product type (Taxonomy based filters) Eg: sourcetype=Firewall
- **data**: Searches the value associated to this variable in the text of the original event. Eg: data="Failed Password"



It is possible to deny any of the above variables to show only events that do not meet the condition defined by the variable, this can be done using != instead of = when assigning the value to each variable. E.g.: data!=root dst!=192.168.1.1

If none of the previous variables are used, the text entered will be searched in every field in all events stored in the Logger.

The different search criteria inserted by the user will be combined if the user creates more than one search condition, if you want to delete any search criteria click on the X next to the criteria you wish to delete.

The system also allows saving the most predefined searches, so they can be easily used in a future analysis.

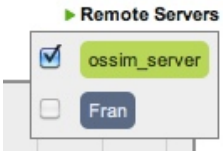
Export

To export the search results to be analyzed using a third-party tool, just mark the **Export** checkbox and click on **Submit Query**

Remote Loggers

You may include more than one Logger in an AlienVault Deployment (Multi-Level deployments). This way the information will be stored at different levels. Using policies the user can configure what is stored in each Logger and what is been forwarded to a Logger running in an upper AlienVault Server.

Information stored in multiple Loggers can be managed with a single Web Management interface. To do this the Loggers must be configured in Assets -> SIEM Components -> Servers. If the Logger is running, it will be shown when clicking on Remote Servers in the Upper right side of the Logger console.



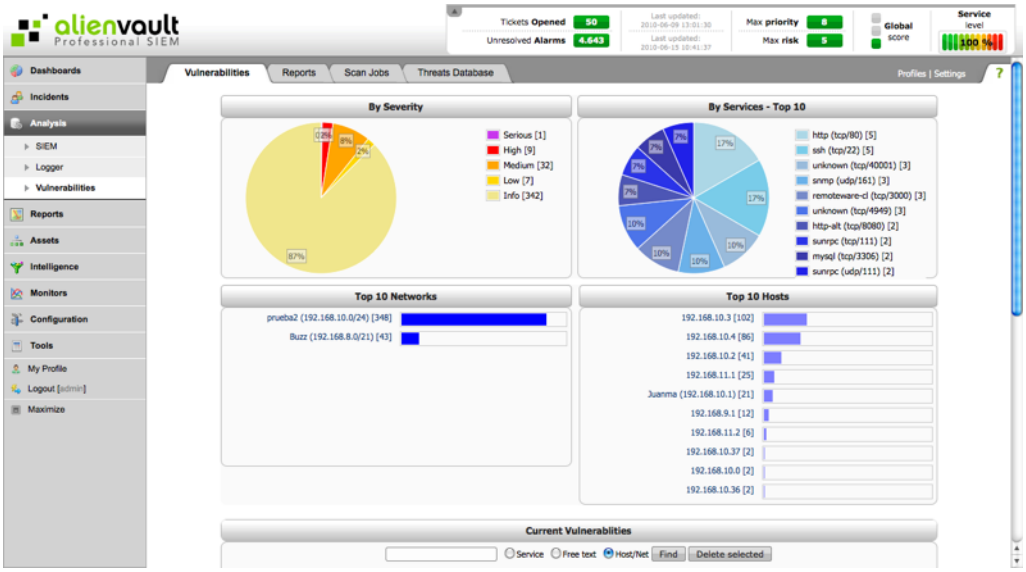
The checkbox next to the name of each Logger will show the events stored in that Logger. Multiple Loggers can be selected at the same time to run searches simultaneously.

Vulnerabilities

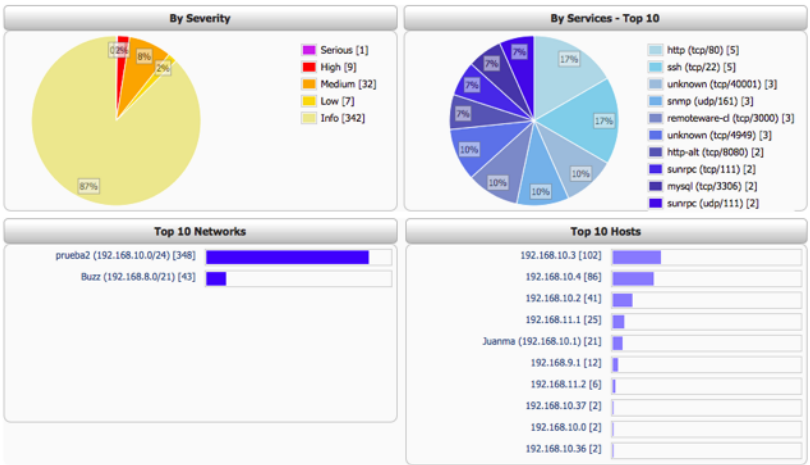
Analysis -> Vulnerabilities -> Vulnerabilities

Description

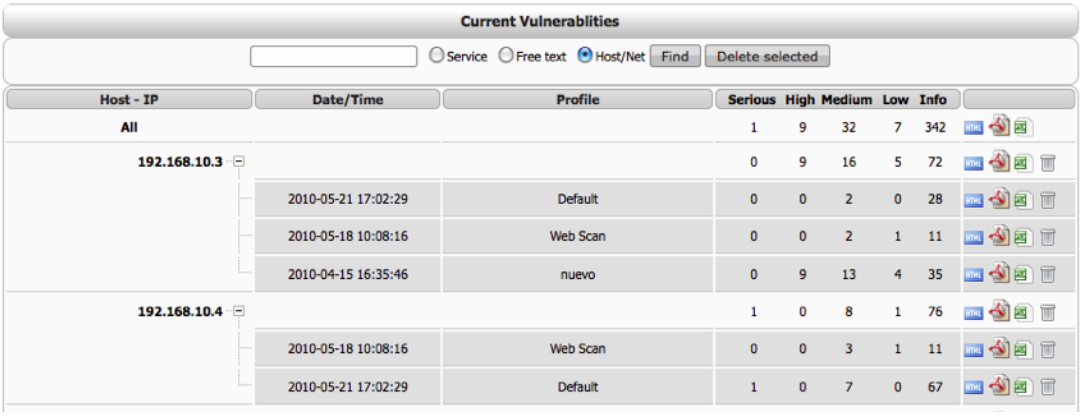
The vulnerability scanning system provides a graphical interface to manage OpenVas and Nessus. The vulnerability scan can be distributed (Vulnerability Scan is done from the AlienVault Sensors) or centralized (Vulnerability Scan from a single location).



In the top you will find graphs generated by the results of the vulnerability scanning process. The graphs show Vulnerabilities by severity, vulnerabilities by services, the most vulnerable networks, and the most vulnerable hosts:



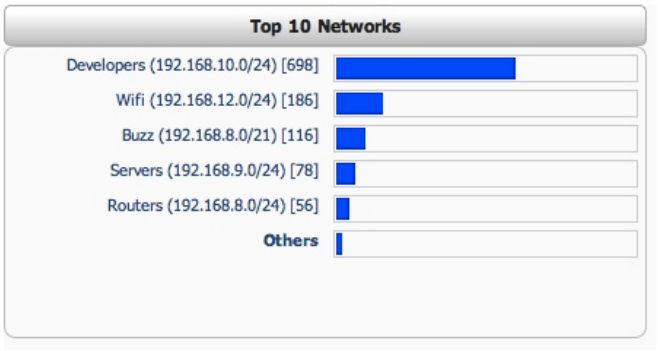
In the bottom, AlienVault shows those hosts and networks that have vulnerabilities, the profile column shows which scanning profile was used to do the vulnerability scanning against the host.



Vulnerabilities are classified based on their severity. Reports can be viewed in PDF, Excel and HTML format.

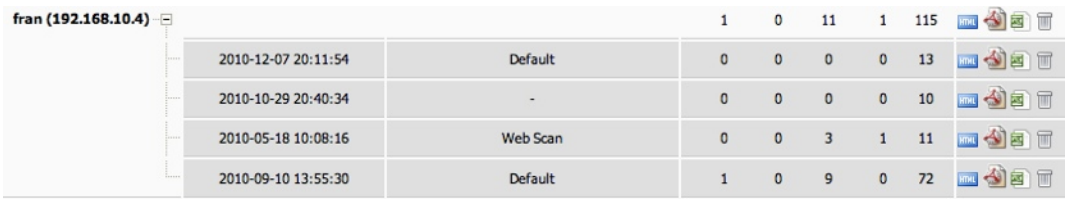
Usage

This tab displays a series of charts showing the results of vulnerability scans that have been executed in the monitored networks. The information displayed is filtered according to the permissions of each user.

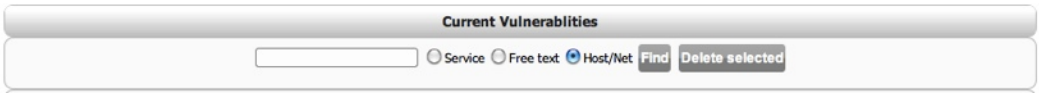


Clicking on the table fields Networks, Top 10 Hosts, or Top 10 reports will show vulnerabilities on the selected network or host.

The table in at the bottom shows the vulnerability scans grouped by host. You can access each of these reports in HTML, .PDF or XLS format.



The Search box in top of the table allows finding vulnerability scanning results with information of a certain service, for a Network or host or even searching some text in all the vulnerability scanning results.

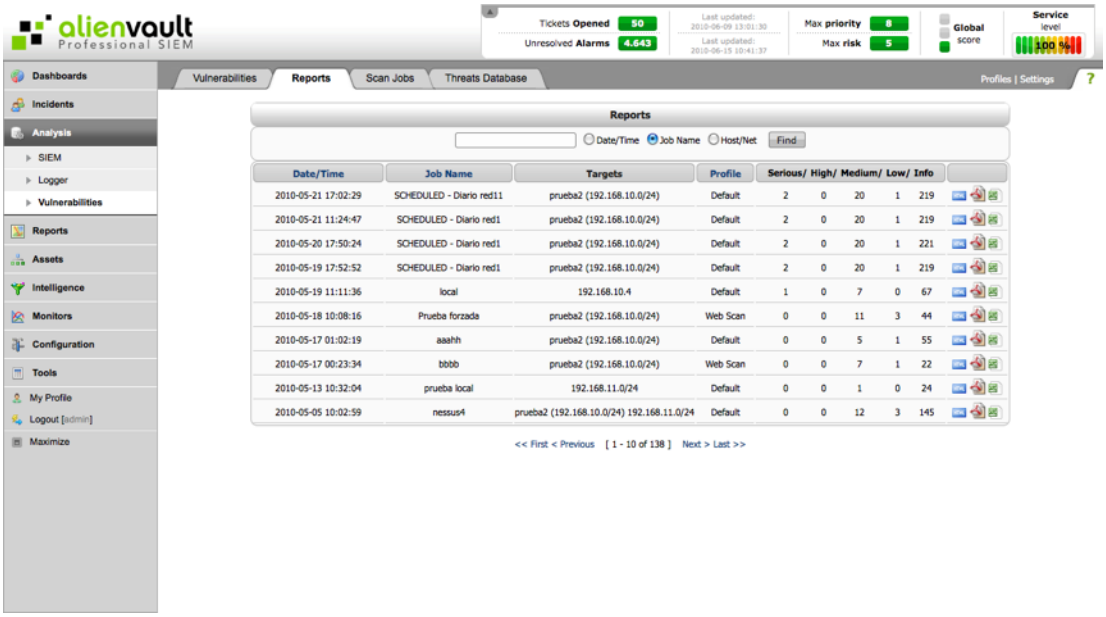


Reports

Analysis -> Vulnerabilities -> Reports

Description

This tab shows the results of the vulnerability scans that have been done in the monitored networks.



From this tab you can also import the results of a vulnerability scan that has been performed using a scanner that is not part of the AlienVault deployment. The report to be imported must be in NBE format, Nessus on Free and Professional versions can generate reports using this format.

Usage

Search Report

You can search for a report by Date/time, scanning job name, or asset that was scanned (Networks and hosts).

View Report

The table will show the following fields for each report:

- **Date/Time**: Date and time when the vulnerability scan started
- **Job Name**: Name given to the vulnerability scanning job
- **Targets**: Hosts or Networks scanned
- **Profile**: Scanning Profile that was used in the vulnerability scanning
- **Serious / High / Medium / Low / Info**: Number of vulnerabilities grouped by risk

Date/Time	Job Name	Targets	Profile	Serious/	High/	Medium/	Low/	Info	
2010-12-07 20:11:54	SCHEDULED - Test nth weekday	fran (192.168.10.4)	Default	0	0	0	0	13	
2010-11-19 09:39:26	Pablo	pablo (192.168.10.2)	Default	0	0	2	0	21	

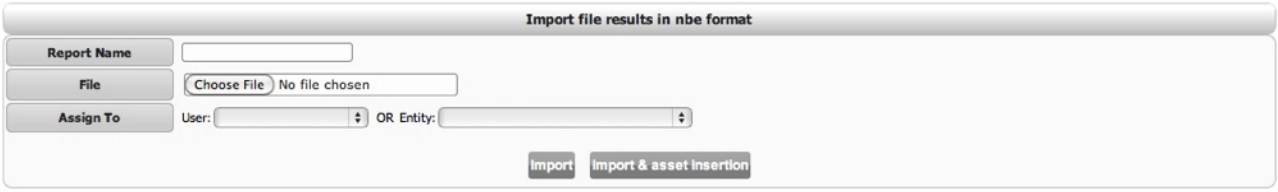
Reports are generated in PDF, Excel and HTML format. To access the report in each different format click on each icon.

When performing a vulnerability scan against a network, the system can discover assets that had not been inventoried in AlienVault. If this occurs, the report would show this icon  . Clicking on this icon will include all the non-inventoried hosts in the report in the AlienVault inventory.

Import Report

Nessus and OpenVas can be configured to export the vulnerability scanning results in NBE format.

When importing a vulnerability scan result, a name must be given to identify the imported result within AlienVault. When importing the report it is also important to configure the users or entities that will be able to see the report.



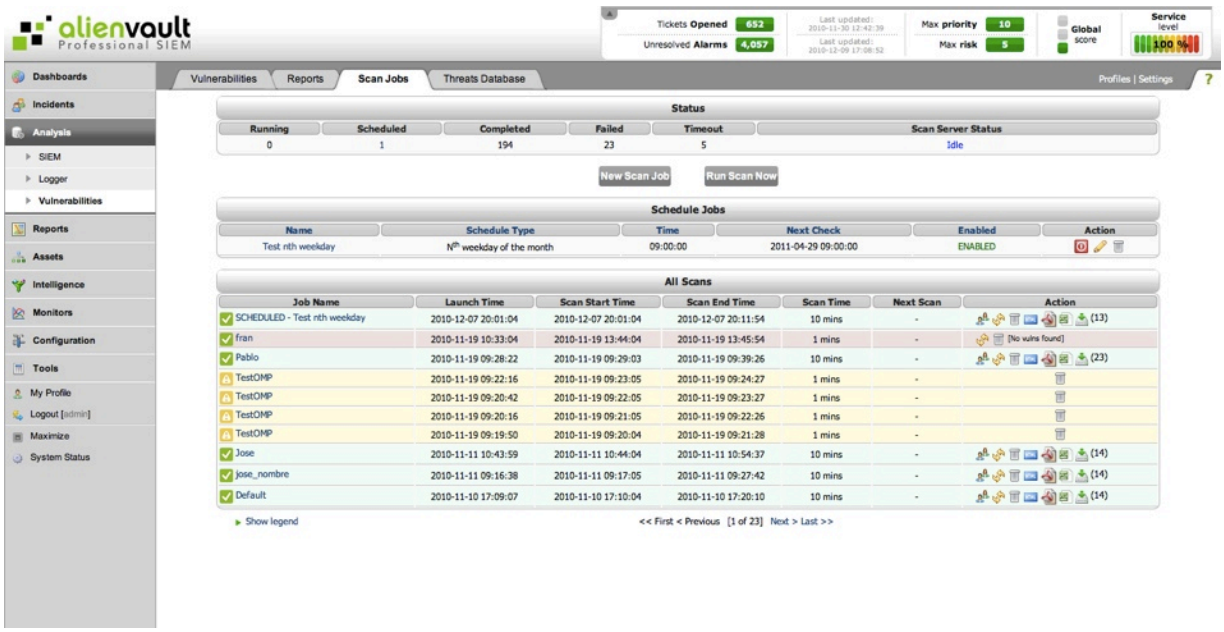
After selecting the NBE that needs to be uploaded, it is possible to just import the vulnerability scanning results or import and insert the non-inventoried assets into the AlienVault inventory.

Scan Jobs

Analysis -> Vulnerabilities -> Scan Jobs

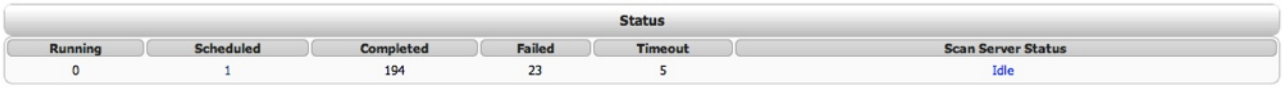
Description

The Scan Jobs tab is used to run or schedule Vulnerability Scanning Jobs as well as to manage the scans running in real time or the previously scheduled Jobs.

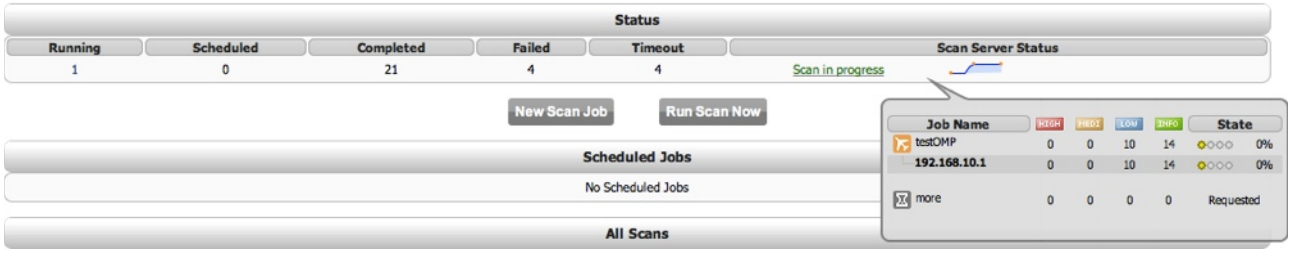


Status

The Status table shows the status in real time of the Vulnerability scanning server. The table includes the number of scheduled scans, scans that were completed, scans that failed, and scans that were not completed because they timed out.



When the vulnerability scanning server is running a scan the table will show a graph representing the number of vulnerabilities that have been found during the scan. If the mouse is over the graph it will show the detail of the vulnerability scanning happening in real time.



Scheduled Jobs

The Scheduled Jobs table shows scheduled scans to be executed periodically, as well as those scans that have been programmed to be executed once, and their executions are pending.

Scheduled Jobs

Name	Schedule Type	Time	Next Scan	Status	Action
Wireless Devices	Monthly	13:30:00	2010-12-15 13:30:00	Enabled	
Web Servers	Daily	15:15:00	2010-12-13 15:15:00	Enabled	

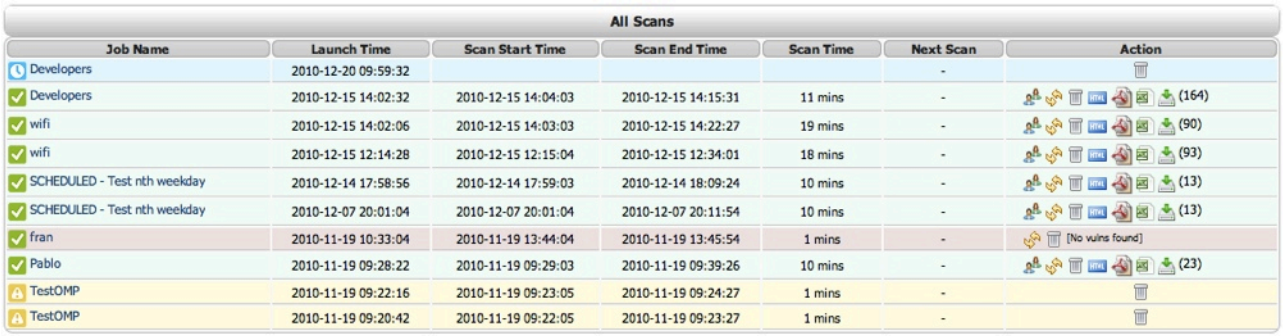
The table will show the following fields for each scheduled job:

- **Name**: Name given to the scheduled job
- **Schedule Type**: Daily / Weekly / Monthly / Day of the month /
- **Time**: Time of the day in which the scan will be done
- **Next Scan**: Time and Date of the next scan of this scheduled job
- **Status**: Enabled or Disabled
- **Action**: Disable the scheduled job . Enable the scheduled job . Edit the scheduled job . Delete the scheduled job .

All Scans

This table shows all vulnerability scans that have run, that are currently running, or that will run in the future. Each Scan Job is displayed using the following fields:

- **Job Name**: Name of the vulnerability Scanning Job
- **Launch Time**: When the vulnerability scan was scheduled
- **Scan Start Time**: When the vulnerability scan started
- **Scan End Time** : When the vulnerability scan finished or timed out
- **Scan Time**: Duration of the vulnerability scan
- **Next Scan**: When the scan will be run again (Scheduled Scans or Scans that failed)



All Scans

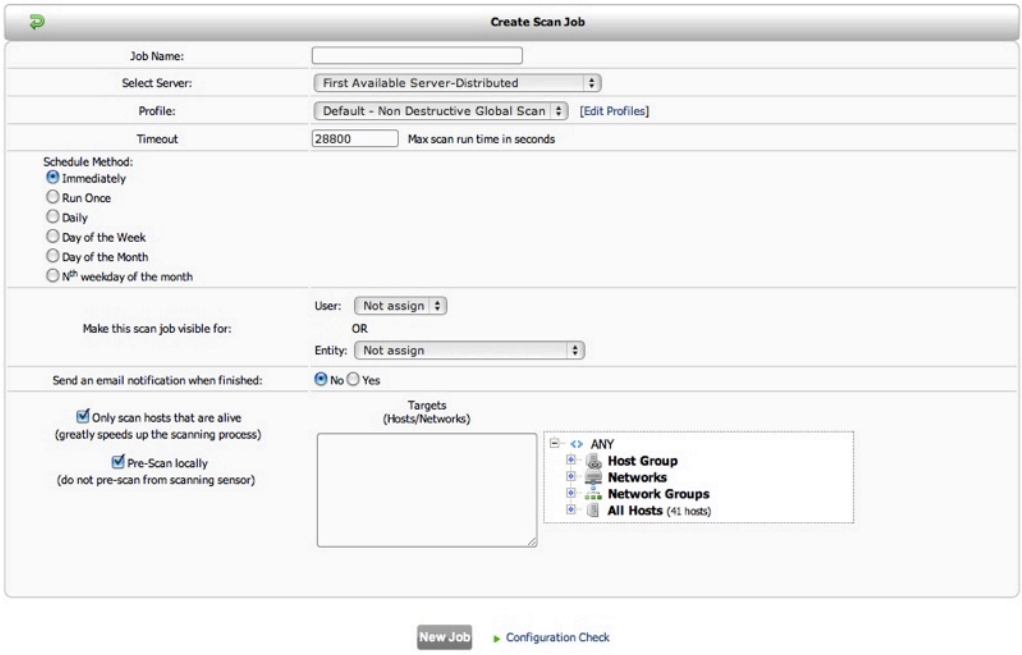
Job Name	Launch Time	Scan Start Time	Scan End Time	Scan Time	Next Scan	Action
Developers	2010-12-20 09:59:32				-	
Developers	2010-12-15 14:02:32	2010-12-15 14:04:03	2010-12-15 14:15:31	11 mins	-	(164)
wifi	2010-12-15 14:02:06	2010-12-15 14:03:03	2010-12-15 14:22:27	19 mins	-	(90)
wifi	2010-12-15 12:14:28	2010-12-15 12:15:04	2010-12-15 12:34:01	18 mins	-	(93)
SCHEDULED - Test nth weekday	2010-12-14 17:58:56	2010-12-14 17:59:03	2010-12-14 18:09:24	10 mins	-	(13)
SCHEDULED - Test nth weekday	2010-12-07 20:01:04	2010-12-07 20:01:04	2010-12-07 20:11:54	10 mins	-	(13)
fran	2010-11-19 10:33:04	2010-11-19 13:44:04	2010-11-19 13:45:54	1 mins	-	[No vulns found]
Pablo	2010-11-19 09:28:22	2010-11-19 09:29:03	2010-11-19 09:39:26	10 mins	-	(23)
TestOMP	2010-11-19 09:22:16	2010-11-19 09:23:05	2010-11-19 09:24:27	1 mins	-	
TestOMP	2010-11-19 09:20:42	2010-11-19 09:22:05	2010-11-19 09:23:27	1 mins	-	

Usage

Scan Jobs

New Scan Job

To configure a new vulnerability scanning job click on **New Scan Job**. The web interface will display a form to configure the scanning parameters.

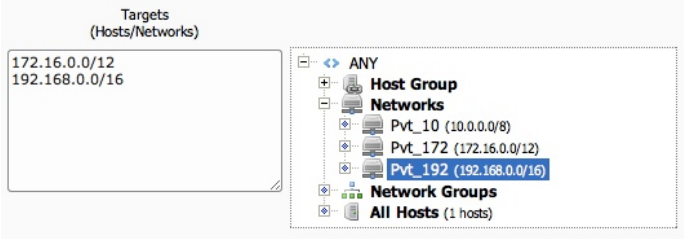


The parameters to be configured are:

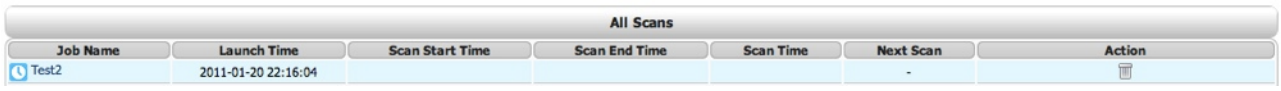
- **Job Name**: Name given to the vulnerability scanning job.Name given to the vulnerability scanning job. If it is a scheduled Job the word SCHEDULED will be added to the Job name.
- **Select Server**: Select the scan server (AlienVault Sensor profile includes the OpenVas Scan Server by default) from which to perform the scan. The scan can also be configured as a distributed scan, this way the system automatically chooses the sensor closest to the host or network being scanned. If no scanning server is selected, the default configuration is “First Available Server - Distributed Scan”
- **Profile**: Vulnerability Scan Profile. Set of OpenVas or Nessus plugins enabled for the scan job.
- **Timeout**: Maximum scan duration. If the scan takes longer the scan will be cancelled.
- **Schedule Method**: Immediately / Run Once / Daily / Day of the week / Day of the Month / Nth weekday of the month
- **Make this scan job visible for**: Users or Entities that will have access to the scan job configuration and to the reports generated by the scan job
- **Send an email notification when finished**: Enable / Disable sending an email to the user who scheduled the scan job once the scan is complete.
- **Only scans hosts that are alive**: Does a fast network scan (Ping scan) prior to start the vulnerability scan to find hosts that are alive. This will greatly speed up but prevent vulnerability scanning to find vulnerabilities on computers that are blocking ICMP requests.
- **Pre-Scan locally**: Run the ping scan from the host running the AlienVault Web Interface

To select the targets to be scanned for vulnerabilities, you have to select them from the tree displaying all assets in the AlienVault inventory (Click on the name of the asset to add it as a target). Available targets will be displayed in a tree in the right side, the left side will show a list with assets that have already been selected as targets to be scanned, to expand each of the branches of the tree click on [+], to hide a branch click on [-].

To launch the scan, click on **New Job**, to launch a simulation of the scan (which checks the user's permissions and the availability of the sensors that must perform the scan), click on **Configuration Check**.

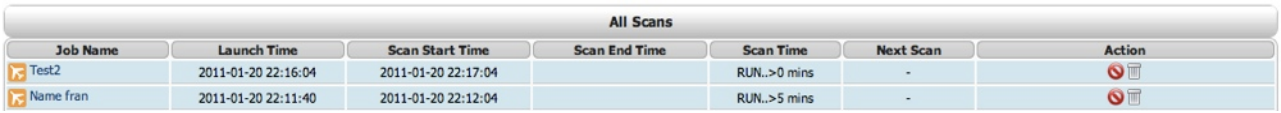


A process checks every 300 seconds if there are pending scans (Scheduled scans that have not been started). For this reason it may take a few minutes before the scans start. Meanwhile, the scan will be displayed in this All Scans table.



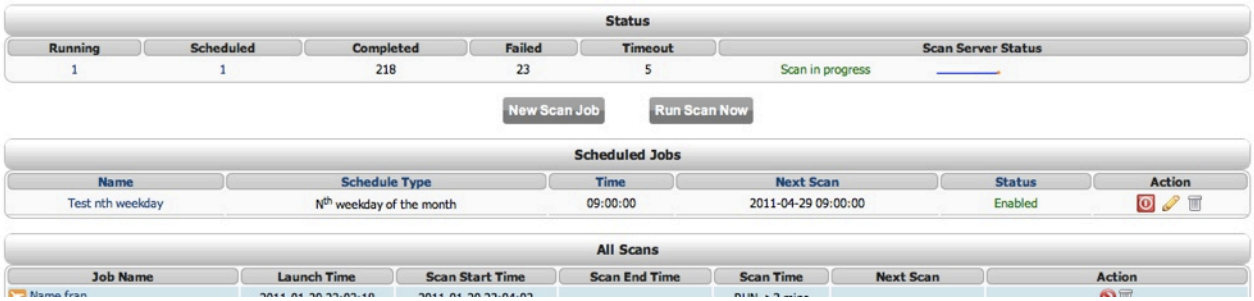
Scheduled scans that have not been started yet will be displayed using this icon:

Running Scans will be shown in the **All Scans** table using this icon



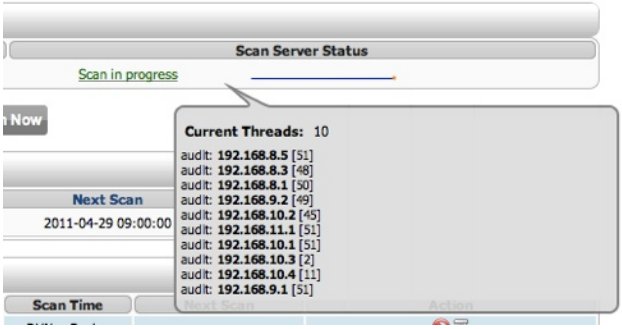
To cancel the Scan Job click on in the line representing the Scan Job that you wish to cancel. To cancel and delete the scheduled job click on .

Once the scan has started you can monitor the status of the Scan Job in the **Status** table.



The blue line next to the text Scan in Progress is a visual representation of the number of vulnerabilities found during the scan.

To see in real time what hosts are been scanned and what plugins are being used place the mouse over the text **Scan in Progress**. This can be useful to find out why an scan takes so long (A lot of targets? Plugins misconfiguration?)



If for some reason the scan fails to start, it will be re-scheduled to be executed again one hour later. After three failed attempts the scan job will be cancelled. Put the mouse over the name of the Scan Job to see wether the scan failed to start or not.

Run Scan Now

The **Run Scan Now** button will allow the user configuring a new scan job to executed immediately.

Re-Run Scan Job

To rerun a Scan Job that was to be executed previously, click on the icon in the line representing the Scan Job that you want to run again (All Scans table). The scan will be executed using its original configuration parameters. (All Scans table)

Delete Scan Job

To delete an Scan Job click on in the line representing the Scan job that you want to delete. This will delete the reports generated by the scan Job (if any) as well as the Scan Job configuration. (All Scans table)

Scheduled Jobs

Delete Scheduled Job

To delete an scheduled Job click on in the line representing the scheduled job that you want to delete. (Scheduled Jobs table)

Modify Scheduled Job

To modify an scheduled Job click on in the line representing the scheduled job that you want to modify. (Scheduled Jobs table)

Enable Scheduled Job

To enable a disabled scheduled Job click on in the line representing the scheduled job that you want to enable. (Scheduled Jobs table)

Disable Scheduled Job

To disable an enabled scheduled Job click on in the line representing the scheduled job that you want to enable. (Scheduled Jobs table)

Reports

View Reports

A report is generated once the Scan Job is finished. Reports are generated in HTML , CSV , PDF and NBE format. To access the reports click on the icon in the line representing the Scan Job in the "**All Scans**" table.

Delete Reports

To delete Vulnerability Scan reports click on in the line representing the Scan job that you want to delete. This will delete the reports generated by the scan Job (if any) as well as the Scan Job configuration. (All Scans table)

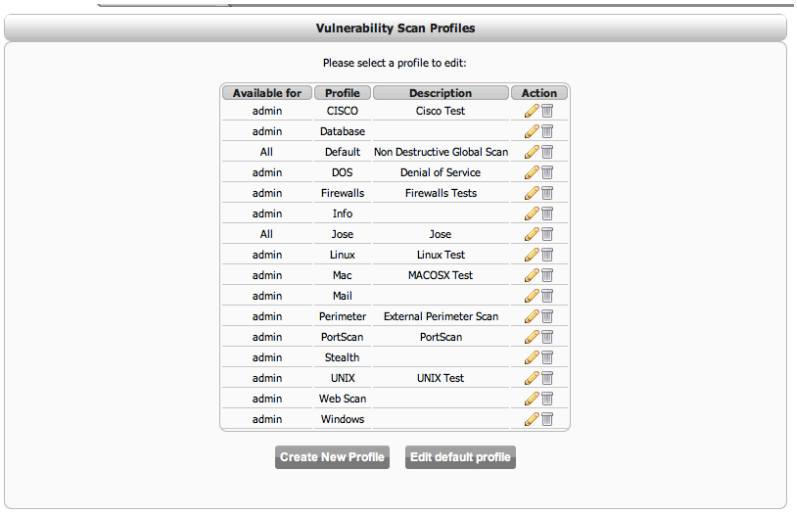
Vulnerability Scan Profiles

The vulnerability scan profiles are the groups of plugins (Nessus or OpenVas plugins) that can be used for vulnerability scanning. AlienVault includes a number of predefined vulnerability scan profiles. Also, users have the ability to create their own.

By creating scanning profiles, the vulnerability scan jobs are greatly accelerated because only plugins that may be useful in our network are used.

It is also possible to create groups of plugins to monitor compliance, enabling only the plugins that are monitoring compliance control objectives.

To access the configuration of the scan profiles click on **Profiles** in the upper right corner.



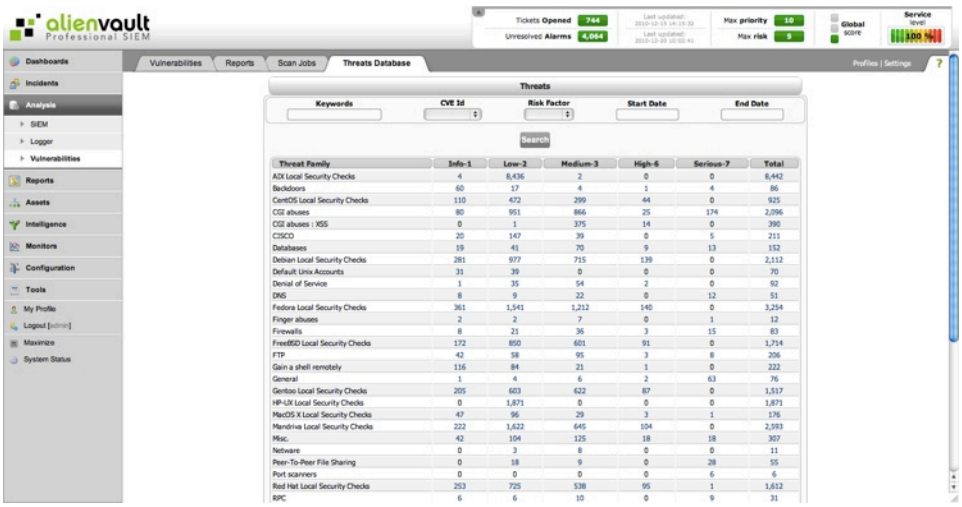
Threats Database

Analysis -> Vulnerabilities -> Threats Database

Description

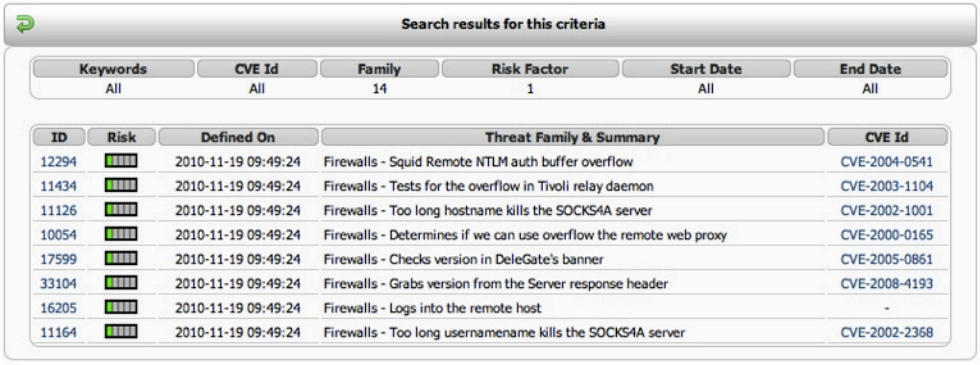
This page displays the vulnerability scanner rules loaded in the database to be used in the vulnerability scans. These rules can be OpenVAS rules or Nessus rules . The default installation includes a set of OpenVAS rules.

The rules are listed grouped by families and by severity.



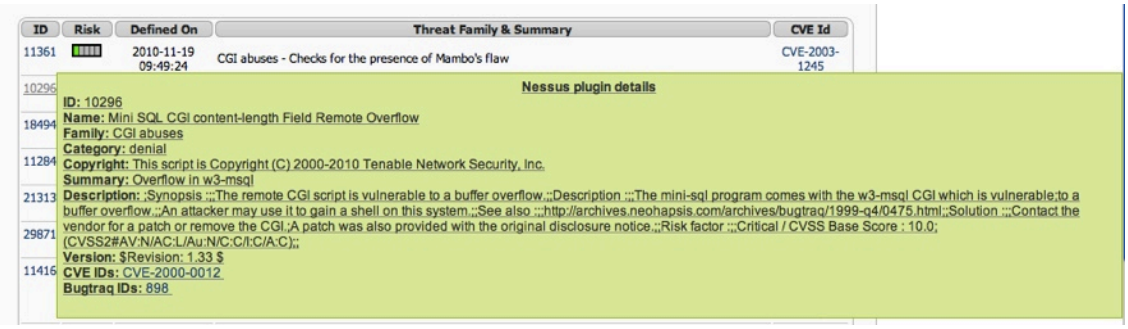
Usage

To access each of the vulnerability scanner plugins, click on the value shown on the Severity columns next to the group of plugins. This will show all plugins belonging to the family with the chosen severity.



Click on  to go back.

To access information of each plugins, put the mouse over the numerical value shown in the ID column.



Most of the plugins contain a CVE identifier referring to the vulnerability that the plugin can detect. Click on the CVE Id in the CVE Id column for more information about this vulnerability.

Search Plugins

A search box is displayed at the top of the page so the user can filter the plugins by keywords, CVE, Risk and by date. Insert your search criteria and click on Search.

Reports

The AlienVault Reporting system offers users the ability to generate complete reports based on the information collected by AlienVault.

The information displayed in the reports is gathered from the SIEM and Logger storage system. When the report is generated the system keeps permissions defined for each user, this way only assets that can be monitored by this user will be included in the report. The user permissions can be changed in Configuration -> Users.

Each report is a combination of sub-reports or modules. The default AlienVault installation includes more than 2000 modules that can be used within reports. Some of them provide enough information to be used as a new report composed by just a single reporting module.

In addition to the default report, each user can easily define new reports without modifying the source code. This is done simply by using a series of forms in the AlienVault Web interface.

For the generation of a new report the user must configure the following aspects:

- Time Window covered by the report
- Assets included in the report
- Sub-reports included in the report,and therefore the sub-reports settings.
- Users and/or entities that may have access to the report

Once a report has been created it can also be scheduled to be generated periodically without user intervention.

Reports are generated in PDF and HTML format.

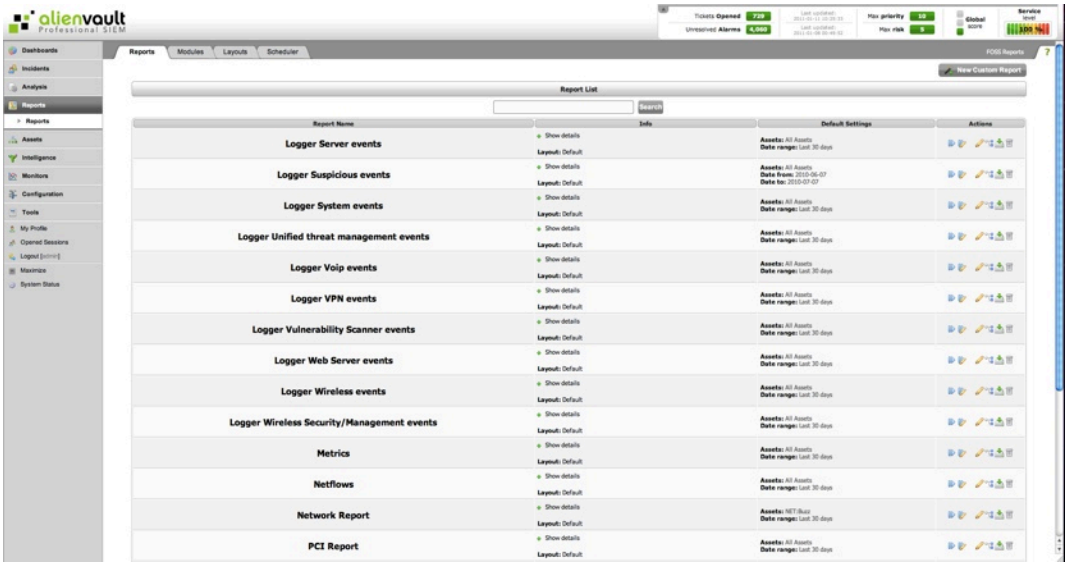
Reports

Reports

Reports -> Reports -> Reports

Description

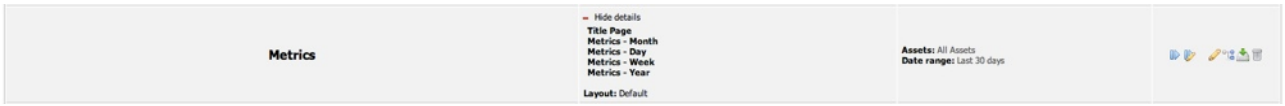
This tab lists all reports that have been configured by the user as well as reports that are included by default when installing AlienVault.



The admin user will see all the reports regardless of who created them. The other users can only view the default reports and the reports that they have created, in case they have permission to create reports.

From this tab you can access the form for creating a new report and generate a report created previously. You can also change the configuration parameters of a report before it is generated.

Each report is displayed in a line. The line shows the name of the report, the contents of the report (reporting modules included), and the configuration of the report, such as assets that appear in the report, layout and date range.



Usage

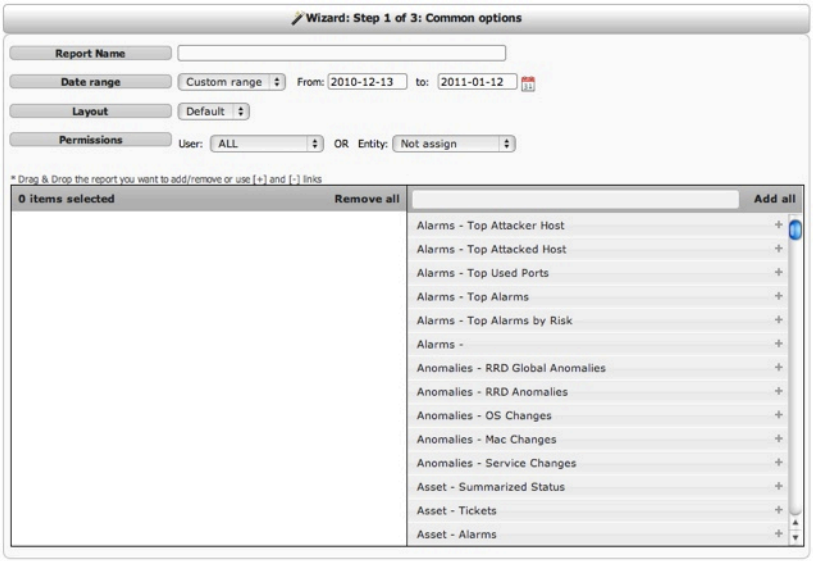
Create a new report

New reports are created using a wizard. In three simple steps you will configure the content and appearance of the new report.

To create a new report click on **New Custom Report** in the upper right side.

In the first step the following aspects of the report are configured:

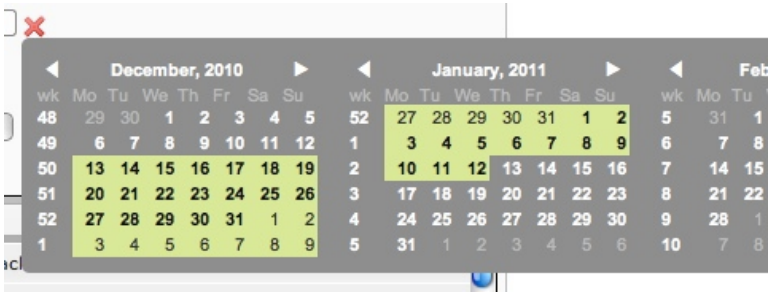
- Report Name
- Date range
- Users and/or entities that will have access to this report
- Layout
- Reporting Modules included in the report



The Report Name can contain alphanumeric characters, spaces and some symbols. This name will identify the report within the report list.

The Date Range determines the time period that will be used to gather the information from the SIEM and/or Logger. To set a date range manually, select Custom Range from the drop menu, and then use the two input box to enter your custom range.

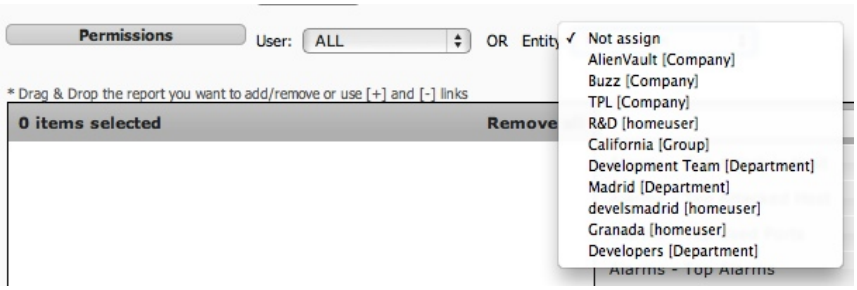
You can also click on this icon to set the date range using a calendar:



If you have created any new layouts, you will be able to select it using the drop menu next to Layout. If not, you can create your own layout if you navigate to Reports -> Reports -> Layout.

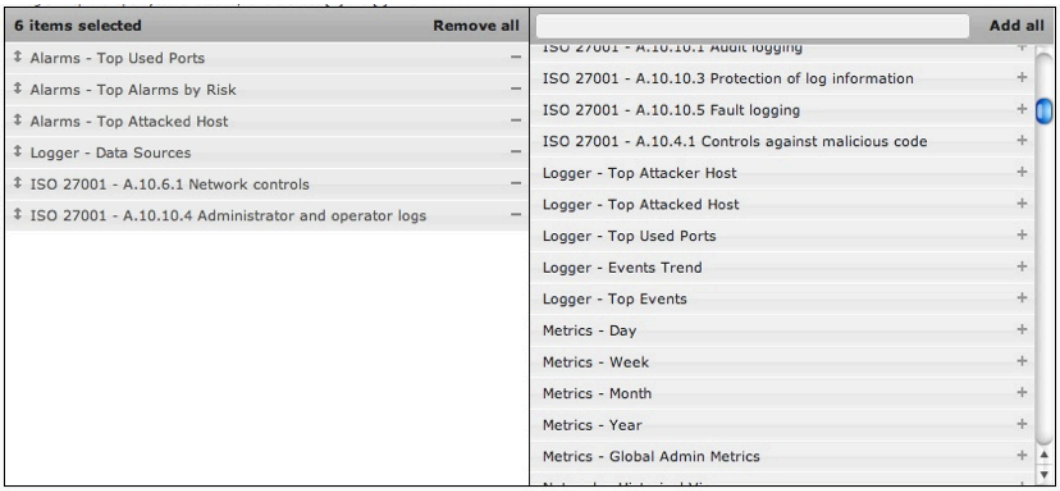
Next you will need to adjust the permissions for this report. By default, each report will be available only to the user who created it and for the admin user, who will always have access to the reports created by all users.

When setting the permissions, you can give access to this report to another user or to an entity. This way, this user or the users within the entity will see this report in their reporting system.



Below is a table of reporting modules available to be included in the report (right side) as well as the reporting modules that have already been included in the report (left side).

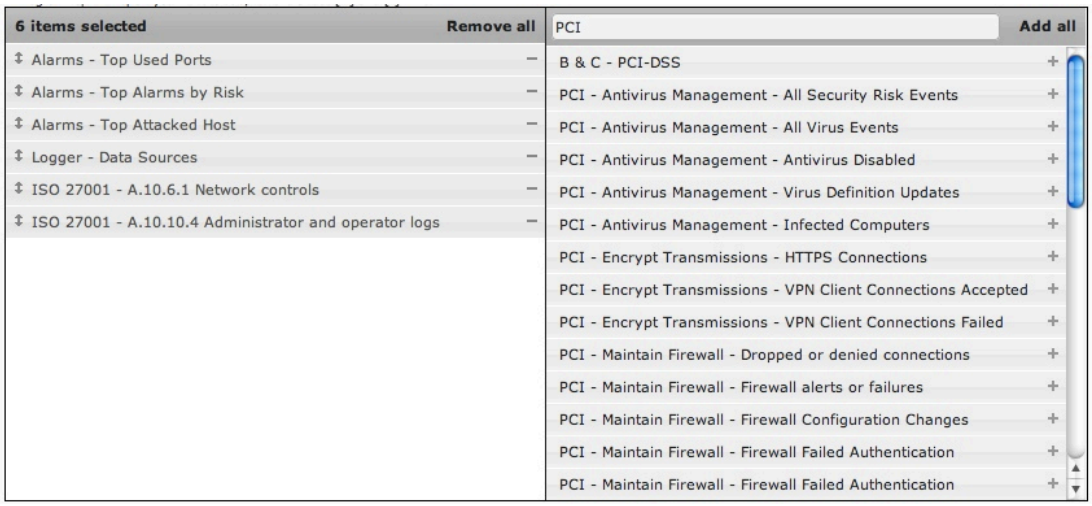
The reporting modules appear in the report in the same order they appear in the table on the left.



To add a new module to the report, drag and drop the module from the right table to the left table or click on [+] next to the name of the module that you wish to include in the report.

To filter between all modules available there is a search box on the right table.

Once the search criteria has been created, drag and drop the module to the left table to include it in the report or click on **Add all** to include all modules that meet the search criteria.



There are some special modules that can be used to include comments or improve the visual aspect of reports such as:

- Page Break
- Title Page
- Comments & Notes

To remove one of the reporting modules click on - next to the name of the report or drag and drop it from the left table to the right table.

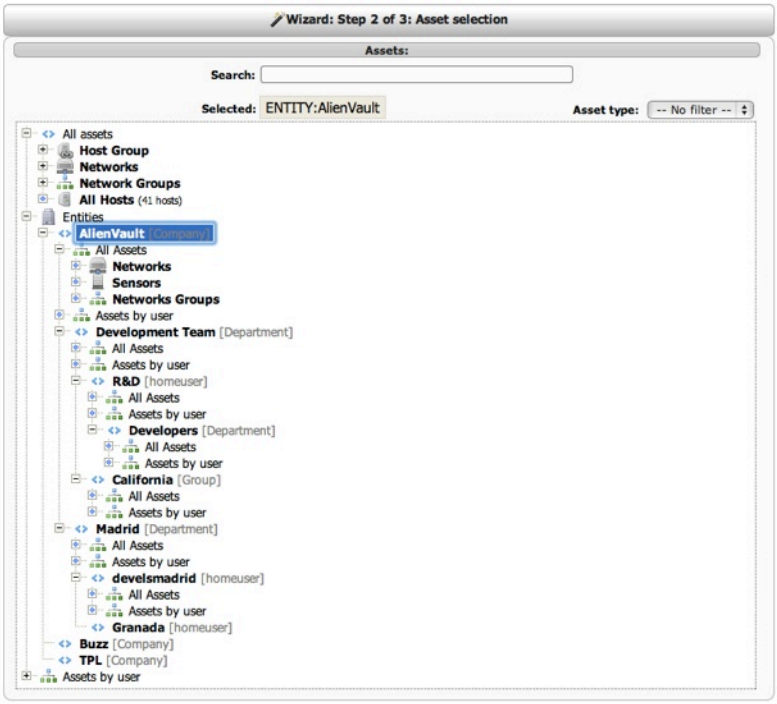
To change the order of sub-reports click the sub-report and drag it to the position where you want it.

Once finished setting the contents of the report click on **Next**.

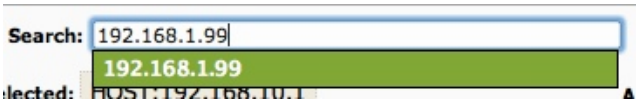
In the second step, select the assets that will appear in the report. All assets in the inventory are displayed using a tree.

If some or your assets are missing from this inventory you will need to update your inventory clicking on Assets in the left menu.

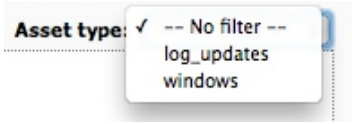
To expand each of the branches of the tree click on **+**. To hide a branch click on **-**



To find an Asset or Entity you can also use the search box on top of the tree. This search box uses auto-completion features.



Assets can also be filtered using the Asset Type filter in the upper right side. This menu will display the search criteria created in the Advanced Asset Search (Assets -> Asset Search -> Advanced).

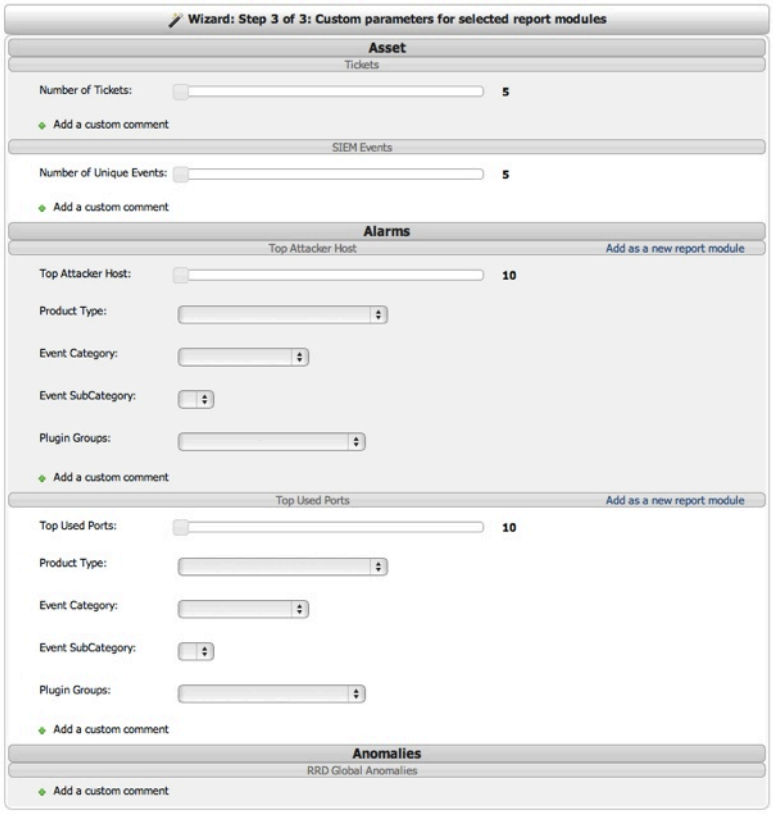


By clicking on the name of the Asset (Network, Network Group or Host) or on the name of the entity, the report will be generated based on the information stored for that Asset or Entity.

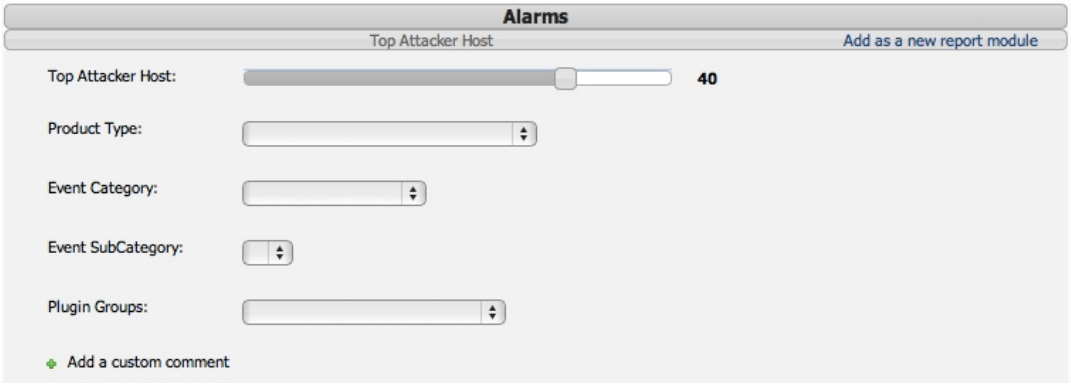
Once you click on an Asset or Entity you will see the selected object on the top of the tree..

By default all Assets in the inventory will appear in the report. Click on **Next** once you have selected the Assets that should be included in the report.

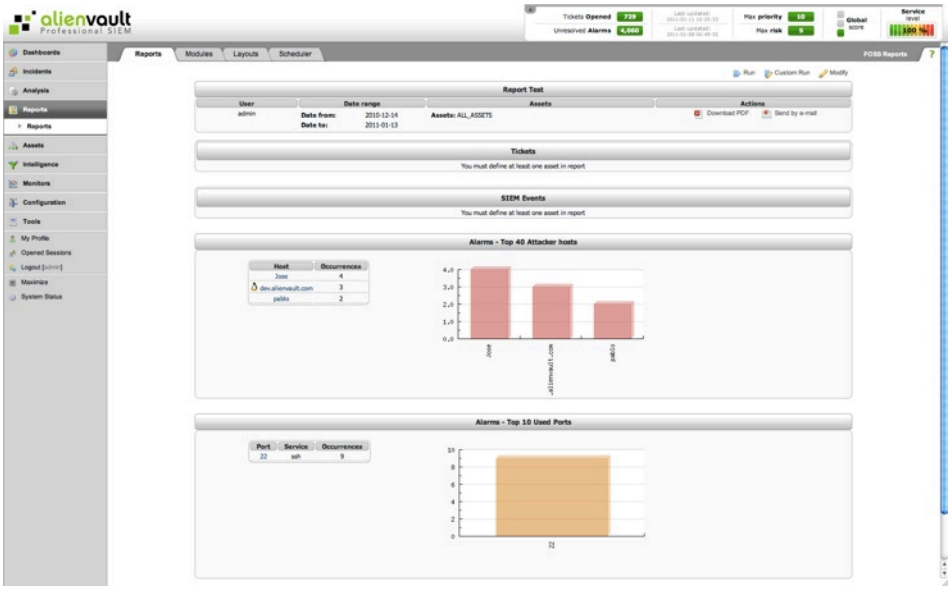
The last step before the report is configured allows for setting the configuration parameters for each reporting module. Depending on the reporting modules that have been included in the report you will be able to set some parameters or even include some text (In case you have included the “Comments & Notes” reporting module). Some reporting modules do not have a configuration function.



When setting the configuration parameters for some reporting modules, you will be able to save the reporting module and its modified configuration as a new reporting module. To do this, click on **Add as a new report module** next to the name of the report.



Finally click on **Update & Run** to save the configuration for this report and generate the report. In case you do not want to generate the report right now click on **Update**.



The report will be generated in both HTML and PDF format. In the top of the report you will find a summary of the configuration used when generating the report, as well as a link to download the report as a PDF file (Click on **Download PDF**).

To send the report in PDF format by e-mail click on **Send by e-mail**.

Above the summary there are three options Run, Custom Run and Modify.

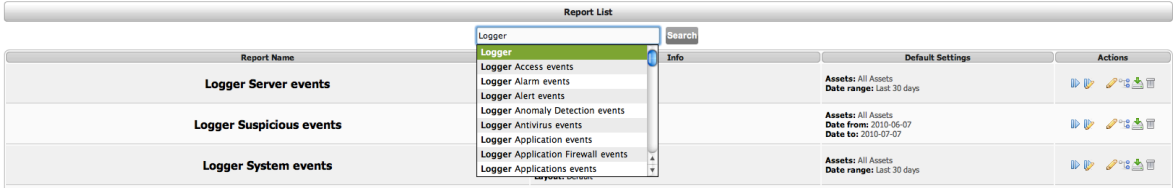
Clicking **Run** will generate the report without changing any of the settings.

Clicking **Custom Run** will generate the report giving the user the possibility changing some settings of the the report. These settings are not saved and will only be used the first time you generate the report using the **Custom Run**.

Clicking on **Modify** you can change the settings of the report without actually running it.

Run a report

To generate one of the existing reports which are included by default or have already been created, you need to find the report in the list of reports. To facilitate this task, there is a search box on top of the list of reports. This search box uses auto-completion features.



Once you have located the report, generate the report with its original settings by clicking on the icon 

To generate the report after changing the original settings click on the icon  . Settings will not be saved.

Modify a Report

To modify a report locate the report in the reports list and click on the icon  . Please refer to the instructions on how to create a New Report.

Clone a Report

To clone a report locate the report in the reports list and click on the icon  .

Export a Report

To export a report locate the report that you wish to export in the report list and click on  .

Import a Report

To import a report that has been created in a different AlienVault deployment click on **Import Custom Report** in the bottom of the list of reports.

Delete a Report

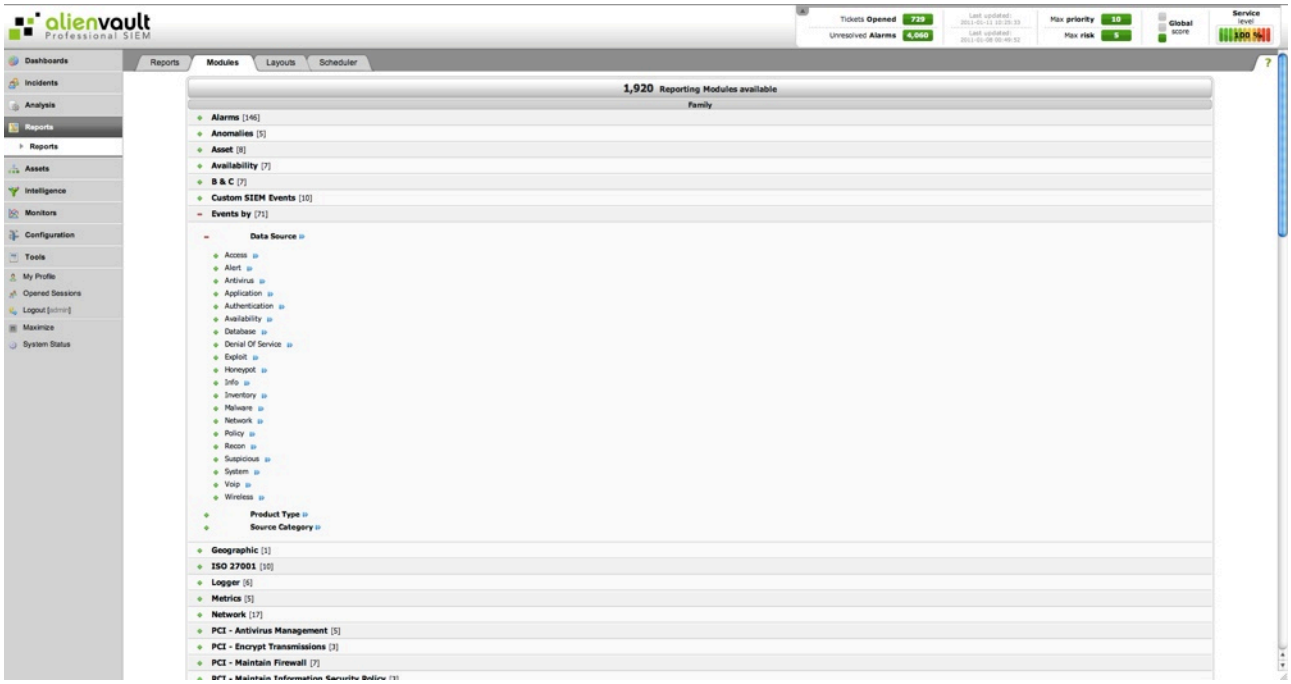
To delete a report locate the report that you wish to delete in the report list and click on  .

Modules

Reports -> Reports -> Modules

Description

The Module section shows a list of all the reporting modules available in AlienVault. These modules have been preconfigured using all possible values that can be used in the settings of the report.



As an example, a reporting module that allows to choose the product type (Taxonomy) in its configuration. This tab will display a list of preconfigured reporting modules using each of the values that can be used in product type configuration parameter.

Usage

The different configuration options offered by each reporting module are shown using a tree, to expand each of the branches of the tree, click on [+]. To hide a branch click on [-].To launch the Wizard Report from one of the reporting modules click on the blue icon.

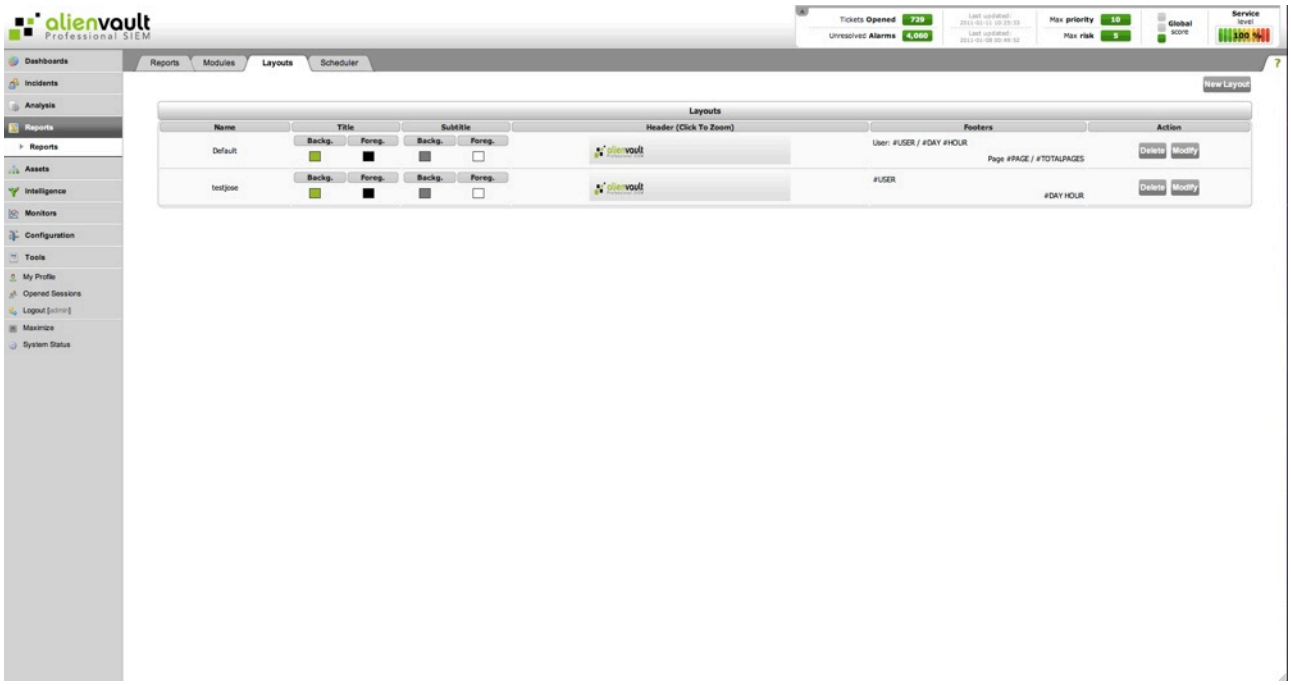
To launch the Wizard Report from one of the reporting modules click on the icon 

Layouts

Reports -> Reports -> Layouts

Description

The layout tab allows you to create different layouts to be used as a template in the reports. A layout can be created to be used within the reports integrating the company corporate logo. You can create as many layouts as needed.

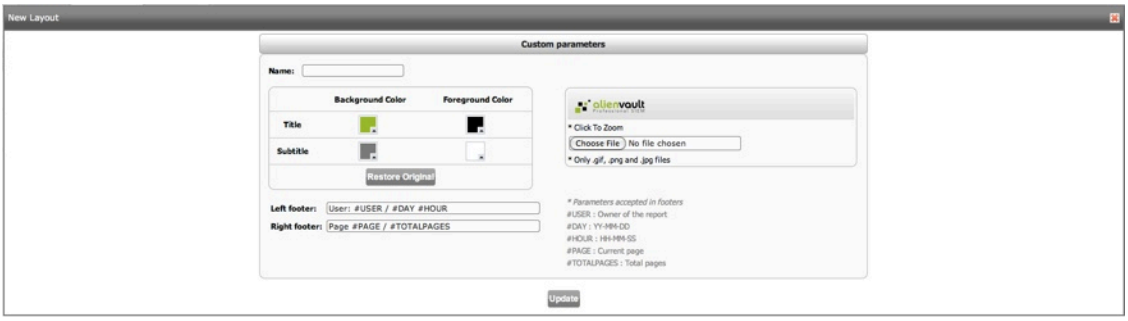


The layout is selected when adjusting the settings of the reports.

Usage

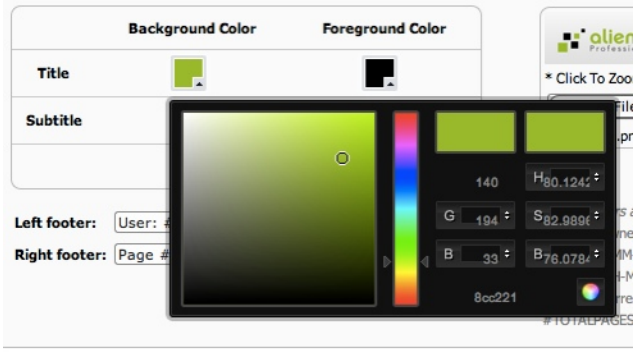
New Layout

To create a New Layout click on **New Layout** in the upper right side. This will show a floating window as shown in this image:



The name of the Layout is a mandatory field that helps identifying this layout.

To change the colors used within this layout click on the color window in the Background Color or Foreground Color columns.



The footer of each page (Not for the Title Page) can be changed using the following keywords:

- **USER**: Owner of the report
- **DAY**: YY-MM-DD
- **HOUR**: HH-MM-SS
- **PAGE**: Current page
- **totalpages**: Total pages

These keywords will be replaced by the value of the variable referred to when generating the report.

The header of each page can be changed using an image in gif, png or jpg format. The image must have dimensions of 1240x128 pixels. To upload a custom image click on **Choose File** and upload your own file.

Once the layout has been configured click on the **Update** button in the bottom to save the new layout.

Modify Layout

To modify a layout locate the layout in the list of layouts and click on the **Modify** button. To modify a layout use the procedure that explains how to create a New Layout.

Delete Layout

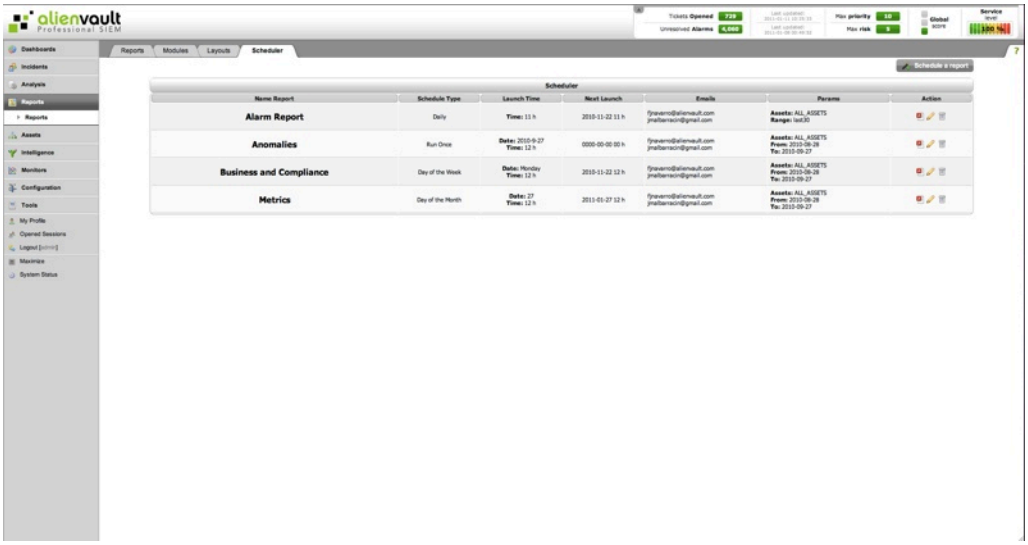
To delete a layout locate the layout in the list of layouts and click on the **Delete** button. The Default layout can not be deleted.

Scheduler

Reports -> Reports -> Schedulers

Description

The reports can be scheduled to be automatically generated periodically. From this tab you can view and modify when the reports are generated.



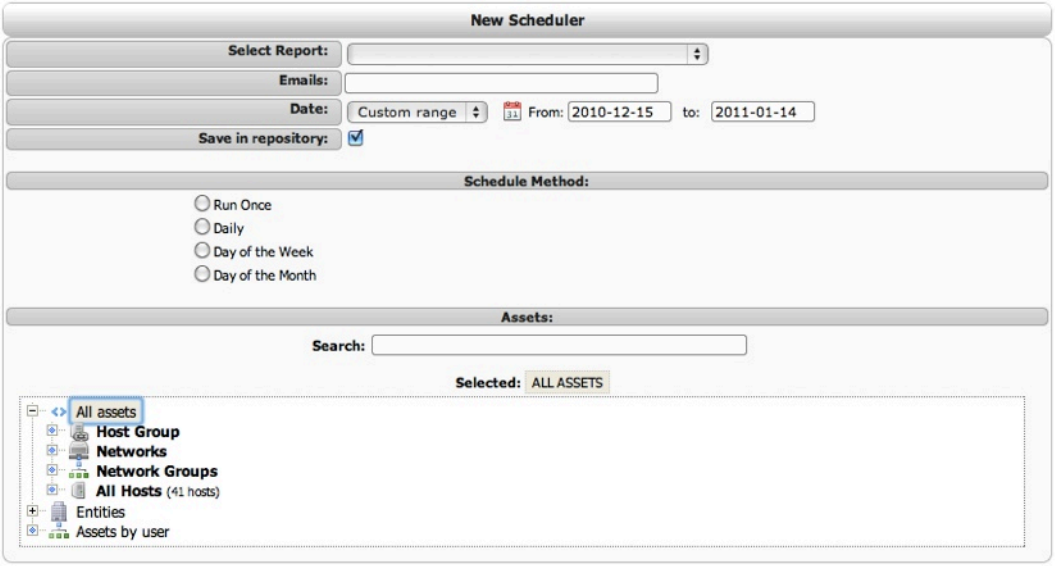
Scheduled reports are listed in a table using the following columns:

- **Scheduled Report**: Name of the report that has been scheduled
- **Schedule Type**: Type of schedule: Daily, Run Once, Day of the Week or Day of the month.
- **Launch time**: Shows the configuration of the schedule type (At what hour will it be generated? What day of the month? What day of the week?)
- **Next Launch**: Shows the time and date in which the report will be generated again.
- **E-mails**: E-mail addresses that will receive the scheduled report.
- **Parameters**: Configuration Parameters (Assets in the report and Date Range)

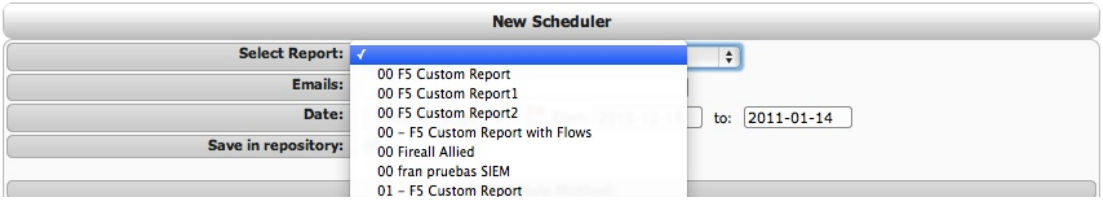
Usage

Schedule a Report

To schedule a report click on **Schedule a Report** in the upper right side of the screen.



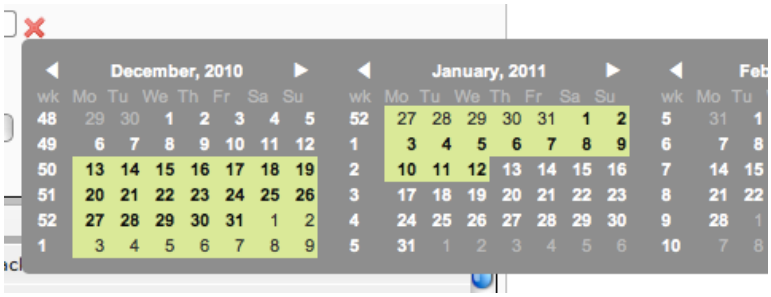
The first thing you have to do is selecting the report that needs to be scheduled. Select the report in the drop-down menu.



If you want the report to be sent to an e-mail address write it in the Emails field. You can use more than one e-mail address separated by semicolon ";".

The Date Range determines the time period that will be used to gather the information from the SIEM and/or Logger. To set a date range manually select Custom Range from the drop menu, and then use the two input boxes to enter your custom range.

You can also click on this icon  to set the date range using a calendar:



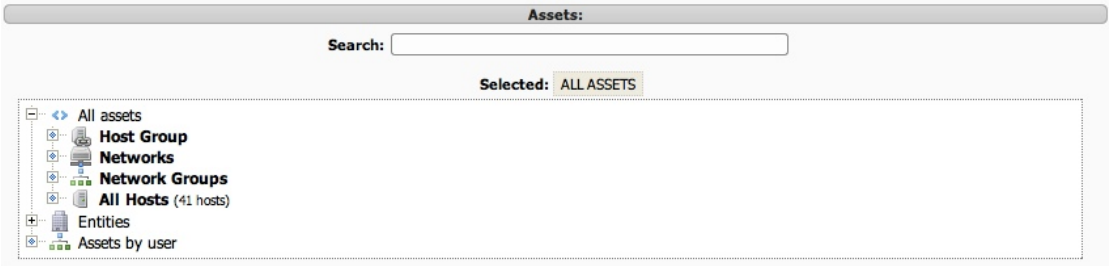
If you want the report to be stored also in the Reports repository to be accessed also using the AlienVault Web interface check the checkbox next to **Save in Repository**.

Select how you want to schedule the report:

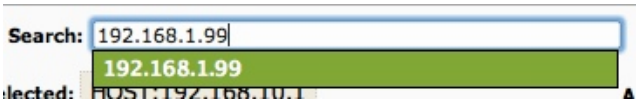
- **Run Once**: Schedule the report to be generated just once
- **Daily**: Schedule the report to be generated everyday
- **Day of the week**: Schedule the report to be generated once a week
- **Day of the month**: Schedule the report to be generated once a month

Select the assets that will appear in the report. All assets in the inventory are displayed using a tree. If some or your assets are missing from this inventory you will need to update your inventory clicking on Assets in the left menu.

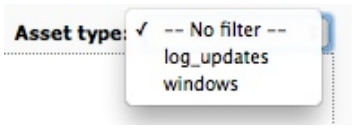
To expand each of the branches of the tree click on **+**. To hide a branch click on **-**



To find an Asset or Entity you can also use the search box on top of the tree. This search box implements auto-completion features.

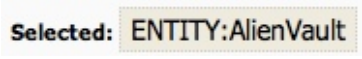


Assets can also be filtered using the Asset Type filter in the upper right side. This menu will display the search criteria created in the Advanced Asset Search (Assets -> Asset Search -> Advanced).



By clicking on the name of the Asset (Network, Network Group or Host) or on the name of the entity the report will be generated based on the information stored for that Asset or Entity.

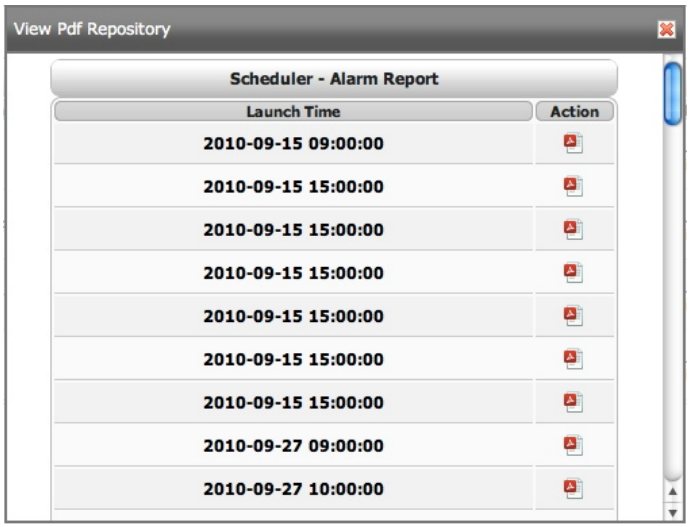
Once you click on an Asset or Entity you will see the selected object on the top of the tree.



By default all Assets in the inventory will appear in the report. Click on **Save Scheduler** to schedule this report.

View Scheduled Reports

To view the scheduled reports that have been generated and stored in the Reports Repository click on the icon next to the report that you would like to download.



A floating window will display all the reports generated by the scheduled Job. Click on the icon to download the report as a PDF file.

Modify a Report Scheduled Job

To modify one the scheduled jobs click on the icon next to the line showing the Scheduled Report Job that you want to modify.

Delete a Report Scheduled Job

To delete one the scheduled jobs click on the icon next to the line showing the scheduled report job that you want to delete.

Assets

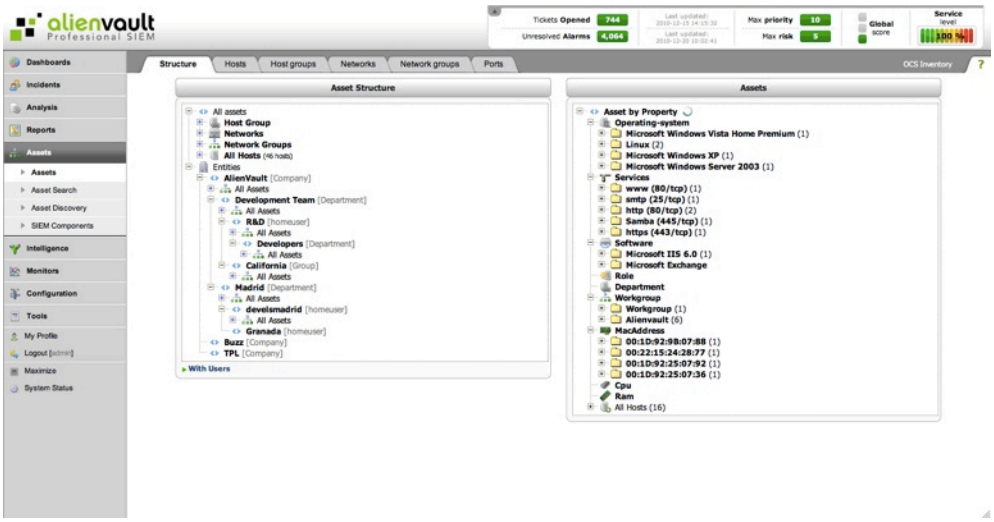
Assets

Structure

Assets -> Assets -> Structure

Description

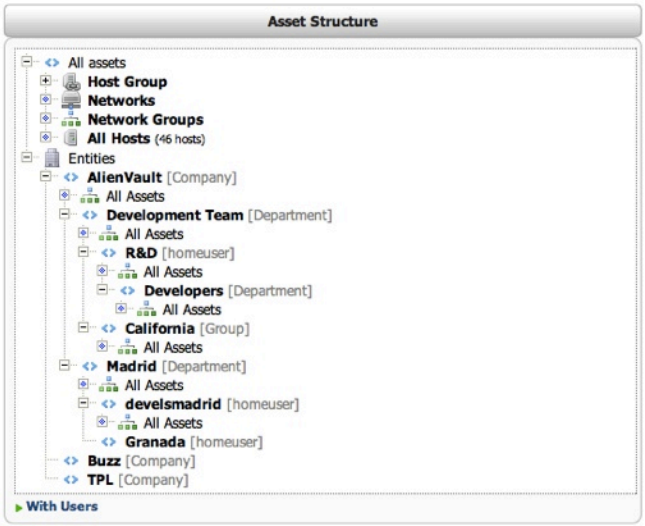
The Structure tab shows all the assets within the AlienVault inventory using a number of trees in which the assets are grouped based on some characteristics of the assets such as Operative System, Services, and Hardware installed in the Asset.



The default view shows two trees. The tree on the left shows the assets grouped by:

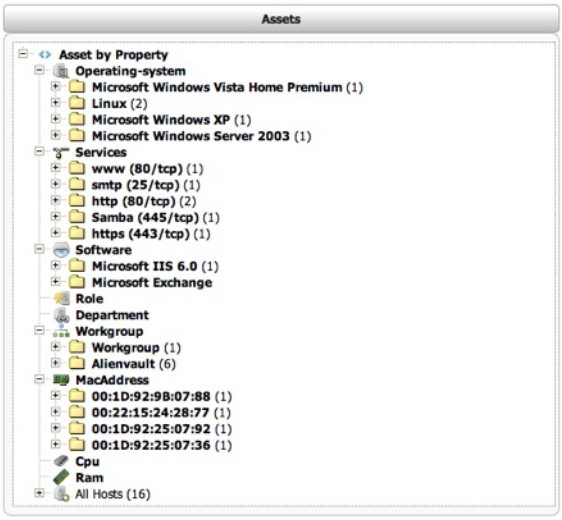
- Host Group
- Network
- Network Groups
- All hosts

Assets are also shown grouped by the entities they belong to.



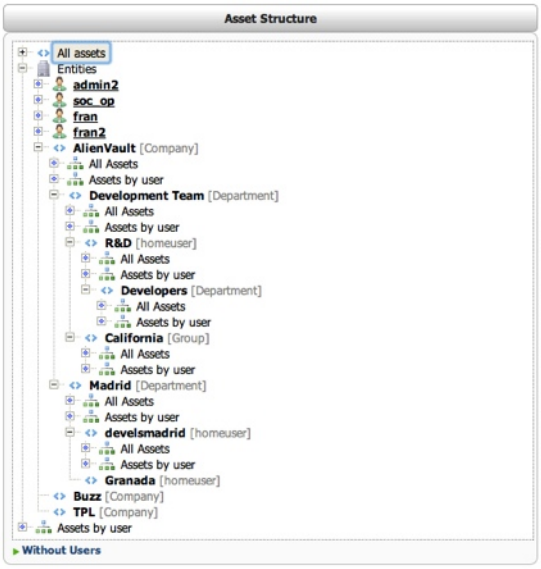
The tree on the right shows the assets grouped by:

- Operating System
- Services
- Software
- Work Group
- Role
- Department
- Mac Address
- CPU
- Ram



Usage

To expand each of the branches of the tree click on **+**. To hide a branch click on **-** . The tree on the left can also include the users within the entity the belong to. To do this click on **With users** at the bottom of the tree.

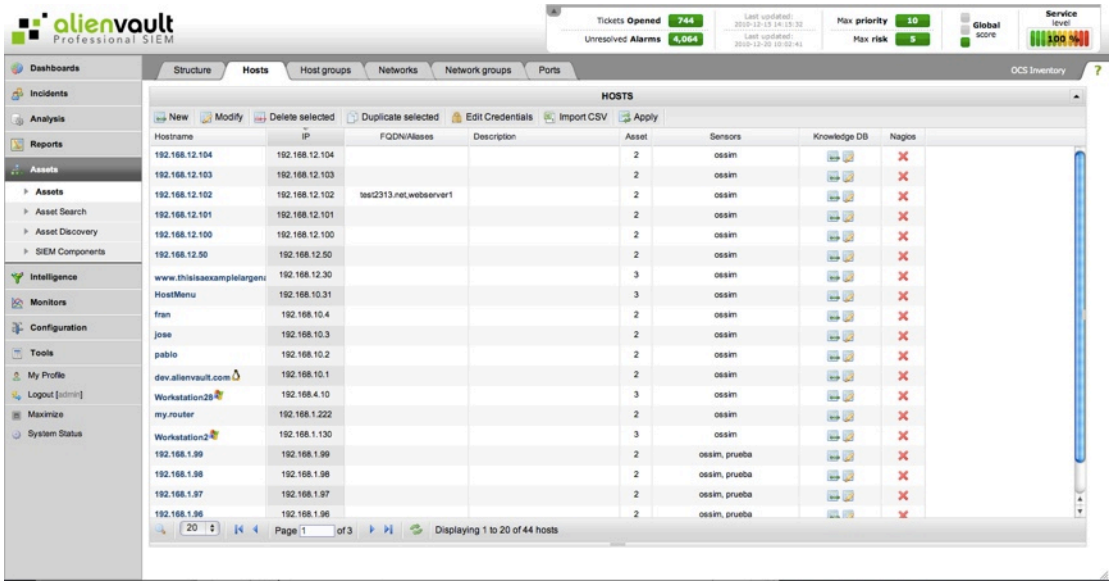


Hosts

Assets -> Assets -> Hosts

Description

This sections offers access to the list of inventoried hosts within AlienVault, certain events will only be stored when the host involved in generating the events belongs to the network that is being monitored. For this reason only assets belonging to the network that is being monitored should be included in the AlienVault inventory.



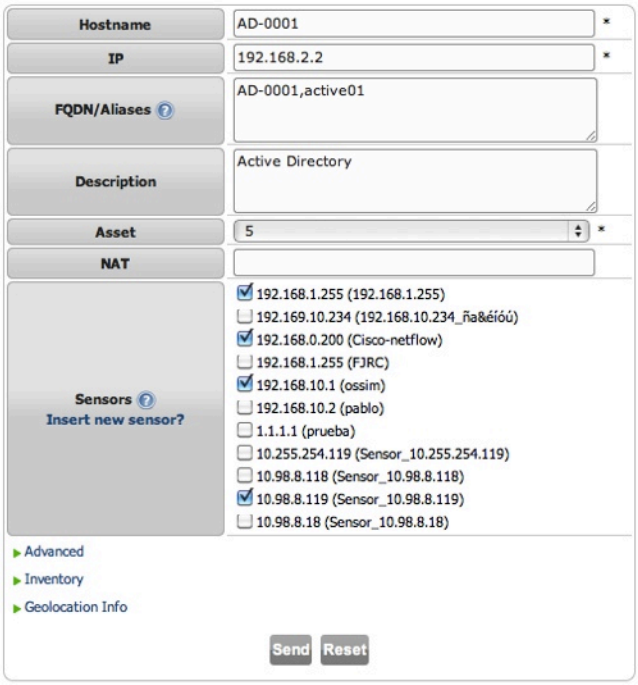
Each host in AlienVault has the following properties:

- **Hostname:** Label assigned to the device (Eg: Web-server)
- **IP:** IP Address in IPV4 format (Eg: 192.168.1.1)
- **FQDN/Aliases**: Fully qualified domain name (FQDN). A host can have more than one alias separated by comma.
- **Description:** Short text describing, for example, the role of the host within the network.
- **Asset Value:** Value given to the host within the network.
- **Sensors:** AlienVault Sensors monitoring the network the host belongs to.
- **Scan options:** Enable/Disable Availability monitoring of the host (Nagios)
- **RRD Profile:** Profile to be used with the RRD Aberrant Behavior Plugin (Anomalies based on information provided by Ntop)
- **Threshold C:** Compromise threshold level
- **Threshold A:** Attack threshold level
- **OS:** Operating System
- **Mac Address**: Unique identifier assigned to network interface
- **Mac Vendor:** Network card manufacturer

Usage

New Host

To insert a new host click on **New** in the upper left of the table:



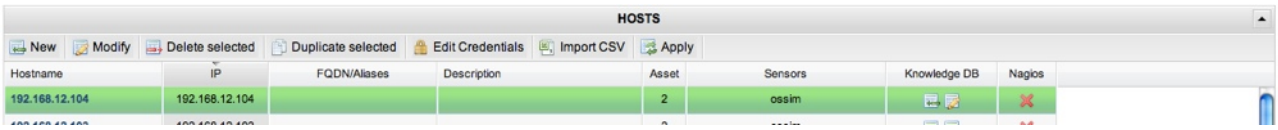
Values marked with (*) are mandatory

Some of the properties of the host must meet special conditions:

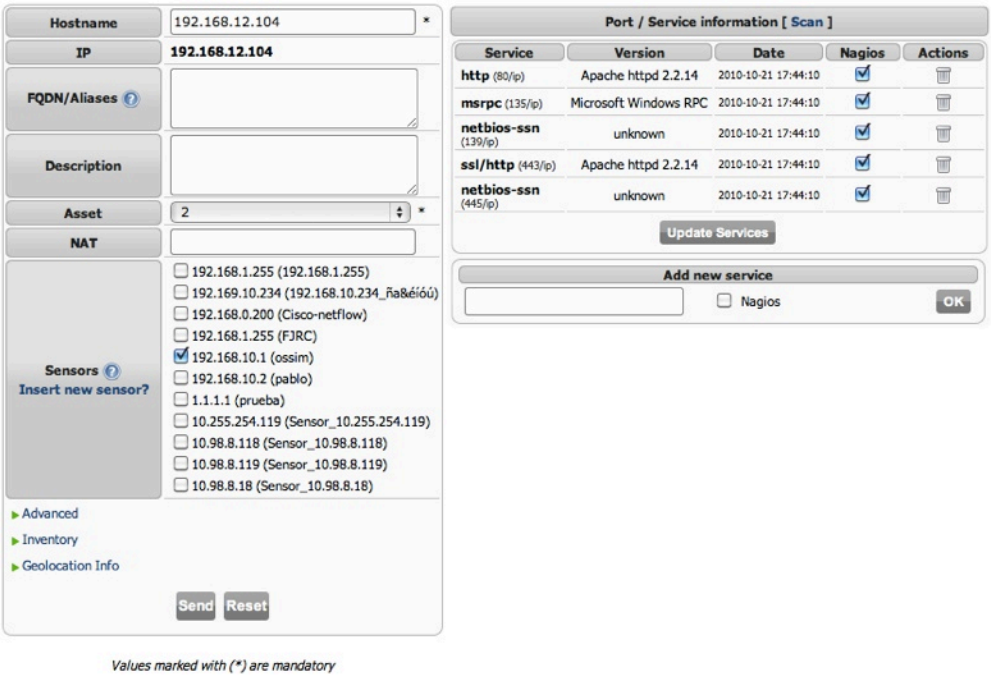
- **Hostname:** Alphanumeric characters with no spaces. Some symbols such as "-" "_" can also be used in the Hostname field.
- **IP:** IP Address in IPV4 format (Eg: 192.168.1.1)
- **FQDN/Aliases**: Fully qualified domain name (FQDN). A host can have more than one alias separated by comma.
- **Description:** Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used.
- **Asset Value:** Numerical value (0-5)
- **Threshold C:** Integer value
- **Threshold A:** Integer value
- **OS:** Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used.
- **Mac Address**: Six groups of two hexadecimal digits, separated by colons (:)
- **Mac Vendo**r: Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used.

Modify a Host

To modify the properties of a Host select the host in the grid using a single left click and then click on **Modify**.

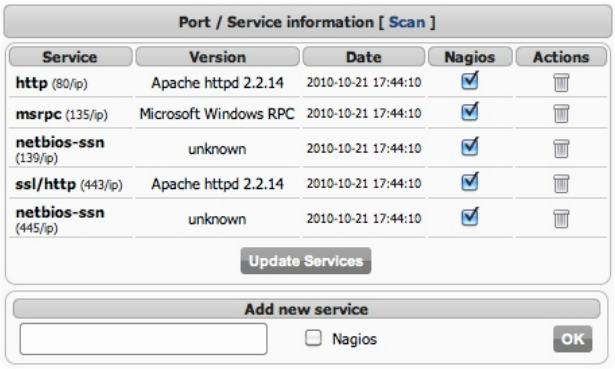


The system will display the following screen allowing you to change the properties of the host.



In addition to the properties described previously, when inserting a host, the system will show a list of services running in the host. Using this list, the system can automatically setup Nagios checks to monitor the availability of the services.

AlienVault automatically populates each host service using the information provided by Pads (Passive Asset Detection System). This information can also be completed using the active scanning tool (Nmap) which can be found at Tools -> Net Discovery



The table in the upper right shows the lists of services of the box, to run an active scan (Using Nmap) in real time to update the list of services click on Scan. The checkbox in the column named Nagios indicates whether AlienVault should automatically configure Nagios to monitor the availability of the service (Checkbox enabled) or not (Checkbox disabled).

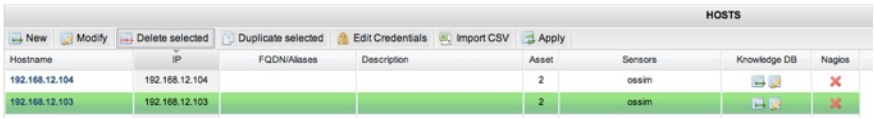
By default, this will be monitored from the Nagios installed in the AlienVault box running the AlienVault Web interface, so make sure that it can access the IP address that needs to be monitored.

If you wish to delete one of the services click on  .

To manually add a new service use the form called Add new service, enter the port and protocol, select wether you want to enable Nagios (Availability Monitoring) for that service or not and click on **OK.**

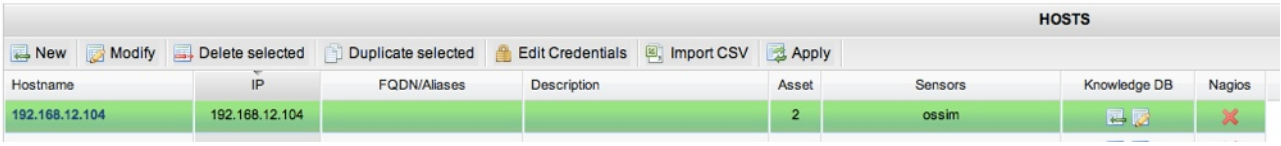
Delete a Host

To delete a host, click on the host (Single left click) and then click on **Delete Selected.**



Duplicate Hosts

To duplicate a host, click on the host (Single left click) and then click on **Duplicate Selected.**



Now you will have the possibility of modifying the properties as if you were inserting a new host.

Edit Credentials

To perform a detailed inventory of software and hardware installed on the host, you can define credentials to log into the host remotely. These credentials will also be used in the future to perform a vulnerability scan taking into account the software installed on each machine that cannot be accessed remotely.

To edit the Credentials of a Host click on the host (Single left click) and then click on **Edit Credentials**.

Select the type of authentication that will be used to log remotely to the host:

- AD (Active Directory)
- SSH
- Windows

Enter the username and password and click on **Update.**

Import CSV

A CSV file containing a list of host can be imported to fill in the AlienVault Inventory. To do this click on **Import CSV**.

The CSV must use the following format:

IP;hostname;FQDNs(FQDN1,FQDN2,...);Description;Asset;NAT;Sensors(Sensor1,Sensor2,...);Operating System

Example:

192.168.10.3;Host_1;www.example-1_esp.es,www.example-2_esp.es;Short description of host;2;;192.168.10.2,192.168.10.3;Windows***

The following Operating systems can be used: Windows, Linux, FreeBSD, NetBSD, OpenBSD, MacOS, Solaris, Cisco, AIX,HP-UX, Tru64, IRIX, BSD/OS, SunOS, Plan9 or IPhone

Apply Changes in Hosts

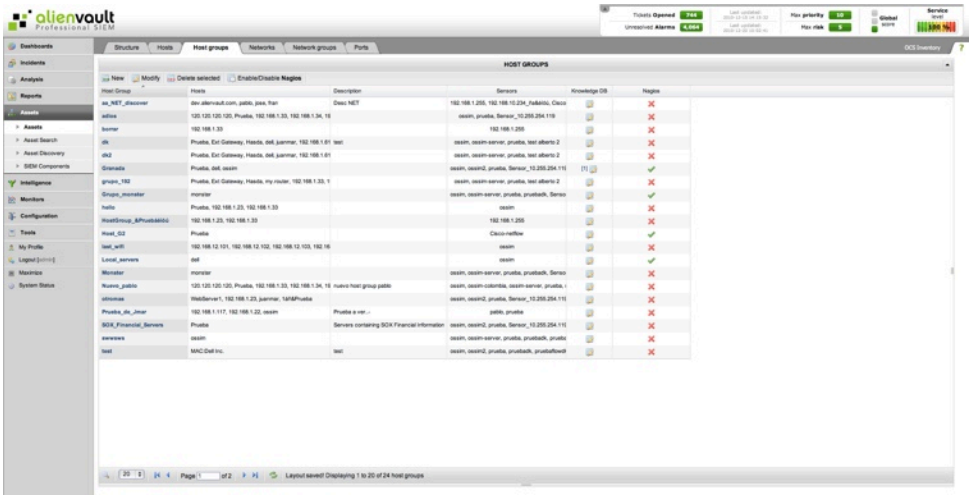
Some properties of the hosts are used when processing the events arriving to the Logger or SIEM. For this reason, once you have finished inserting or modifying the hosts, click on **Apply**. This will reload all hosts information in the SIEM and Logger.

Host groups

Assets -> Assets -> Host Groups

Description

Host Groups are used to create a new object which groups hosts of the same network or different networks. Host Groups can be used to create policy exceptions, run vulnerability scanning against this host group, or to create reports only for hosts belonging to the host group.



A Host Group has the following properties in AlienVault:

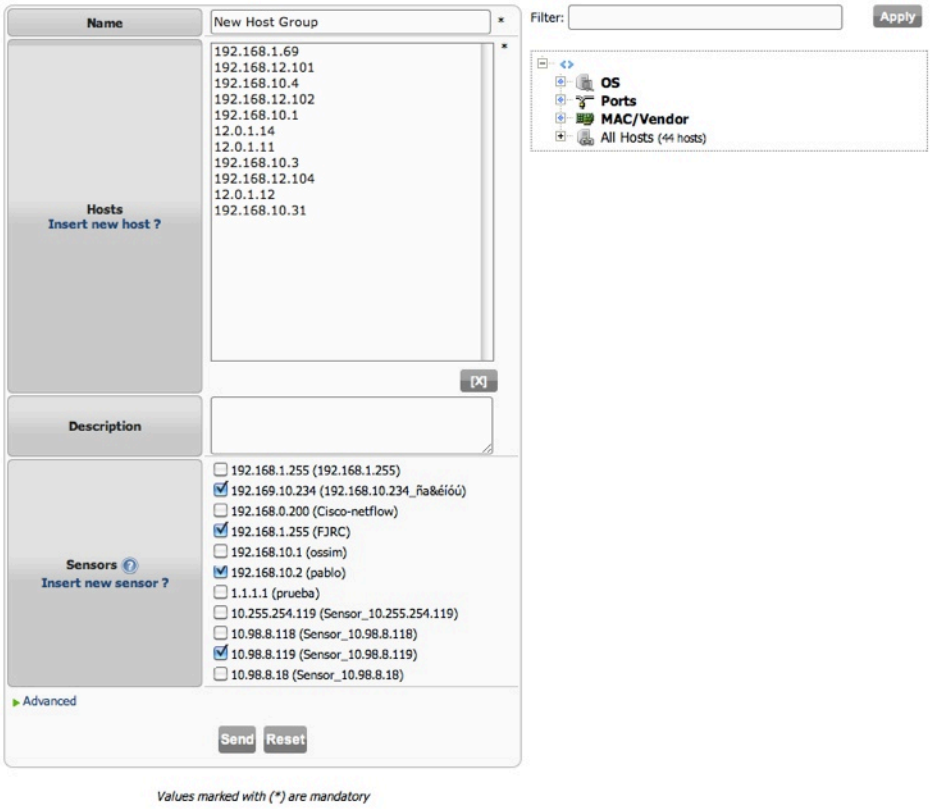
- **Name:** Label assigned to the Host Group (Eg: Web-servers).
- **Hosts:** Lists of hosts in IPV4 format (Eg: 192.168.1.1)
- **Description:** Short text describing, for example, the role of the hosts part of this Host Group. Alphanumeric characters and spaces.
- **Sensors: AlienVault** Sensors monitoring the hosts that belong to the Host Group.
- **Scan options:** Enable/Disable Availability monitoring of the Host Group (Nagios). This needs to be enabled in every host included in the Host Group.
- **RRD Profile:** Profile to be used with the RRD Aberrant Behavior Plugin (Anomalies based on information provided by Ntop)
- **Threshold C:** Compromise threshold level
- **Threshold A:** Attack threshold level

Usage

New Host Group

To create a new Host Group click on **New**.

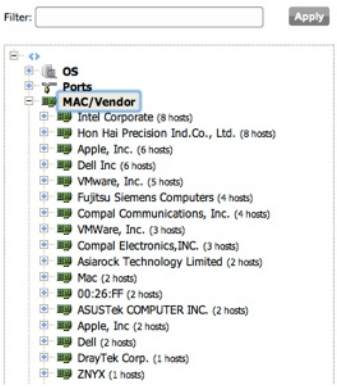
You will have to fill in the following form:



Some of the properties of the Host Group must meet special conditions:

- **Name:** Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used in the Hostname field.
- **Hosts:** Lists of hosts in IPV4 format (Eg: 192.168.1.1)
- **Description:** Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used.
- **Threshold C:** Integer value
- **Threshold A:** Integer value

To insert hosts in the Host Group you can write manually the list of hosts in IPV4 format (one host per line). Hosts to be included in the Host Group can also be selected from the tree on the left.



Above the tree there is a search box that can be used to filter the host appearing in the tree.

Modify a Host Group

To modify the properties of a Host Group select the Host Group in the grid using a single left click and then click on **Modify**.

When modifying a Host Group you will see the same properties that were described previously in the **Insert New Host Group** section.

Delete a Host Group

To delete a Host Group, click on the Host Group (Single left click) and then click on **Delete Selected.**

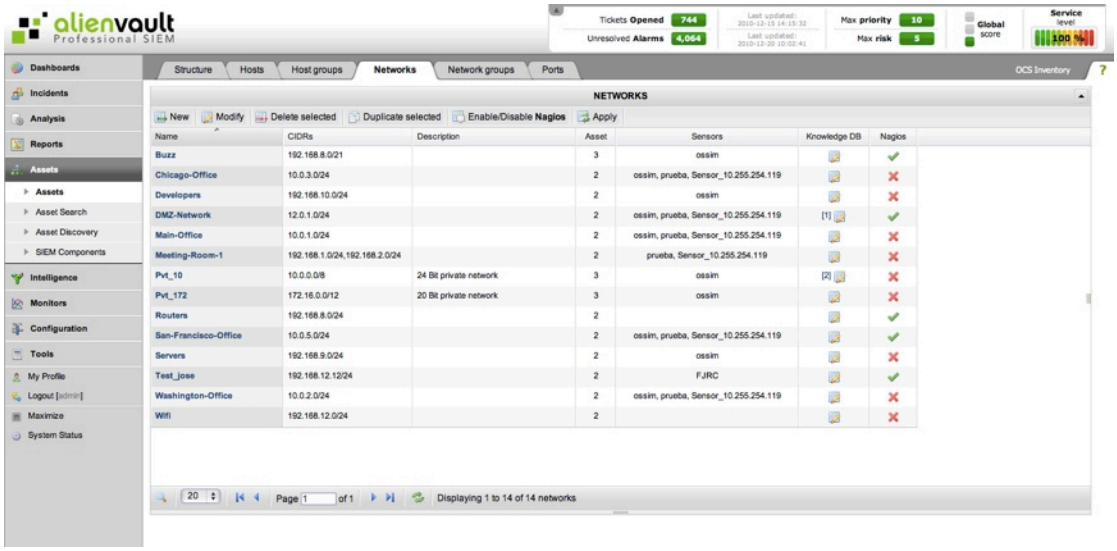
Networks

Assets -> Assets -> Networks

Description

One of the first things that should always be done in AlienVault is the insertion of all the networks belonging to the corporation that will be monitored. This way AlienVault will have an easier time when processing events that have been generated by the local networks.

Each network must be linked with at least one sensor. The sensors linked to the network will be those collecting events or traffic from the monitored network. This is very important as this will be used when setting the user permissions, when generating reports and during correlation.



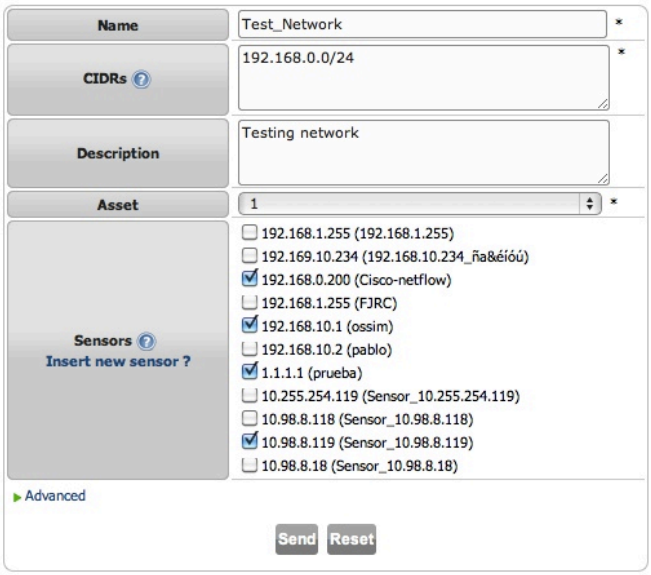
A Network in AlienVault has the following properties:

- **Name:** Label assigned to the Network.
- **CIDRS:** Range of IP Addresses that define the network.
- **Description:** Short text describing, for example, the role of the hosts part of this Host Group.
- **Asset Value:** Value given to the network within the corporation
- **Sensors: AlienVault** Sensors monitoring the hosts that belong to the Host Group.
- **Scan options:** Enable/Disable Availability monitoring of the Host Group (Nagios). This needs to be enabled in every host included in the Host Group.
- **RRD Profile:** Profile to be used with the RRD Aberrant Behavior Plugin (Anomalies based on information provided by Ntop)
- **Threshold C:** Compromise threshold level
- **Threshold A:** Attack threshold level

Usage

New Network

To insert a new Network click on **New** in the upper left side.



Some of the properties of the Networks must meet special conditions:

- **Name:** Alphanumeric characters with no spaces. Some symbols such as “-” “_” can also be used in the Hostname field.
- **CIDR**: IP address and the prefix size, the latter being the number of leading 1 bits of the routing prefix. The IP address is expressed according to the standards of IPv4. It is followed by a separator character, the forward slash (/) character, and the prefix size expressed as a decimal number. (Eg: 192.168.100.1/24)
- **Description:** Alphanumeric characters and spaces. Some symbols such as “-” “_” can also be used.
- **Asset Value:** Numerical value (0-5)
- **Threshold C:** Integer value
- **Threshold A:** Integer value

Modify a Network

To modify the properties of a Network select the Network in the grid using a single left click and then click on **Modify**.

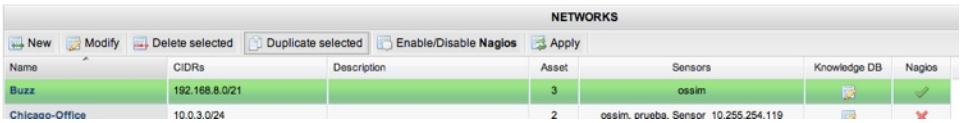
When modifying a Network you will see the same properties that were described previously in the **Insert New Network** section.

Delete a Network

To delete a Network, click on the Network (Single left click) and then click on **Delete Selected.**

Duplicate a Network

To duplicate a Network, click on the Network (Single left click) and then click on **Duplicate Selected.**



Now you will have the possibility of modifying the properties as if you were inserting a new network.

Apply changes in Networks

Some properties of the Networks are used when processing the events arriving to the Logger or SIEM. For this reason, once we have finished inserting or modifying the Networks it is required to click on **Apply.** This will reload all Networks information in the SIEM and Logger.

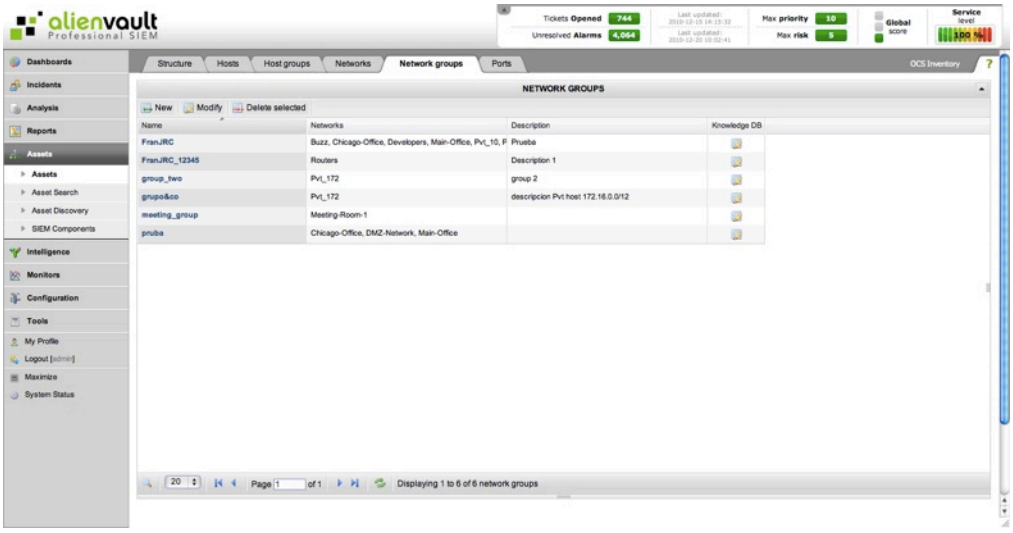
Network groups

Assets -> Assets -> Network Groups

Description

Network Groups are used to create a new object that groups, for example, all the networks from the same corporation in case we are monitoring with a single AlienVault deployment more than one corporation.

In big environments Network Groups can also be used to group all sub-networks around the world with the same role. (E.g.: All servers network, all the wireless networks...) Network Groups can be used to create policy exceptions, to run vulnerability scanning against this network group, or to create reports including the information of all hosts that belong to a Network Group.



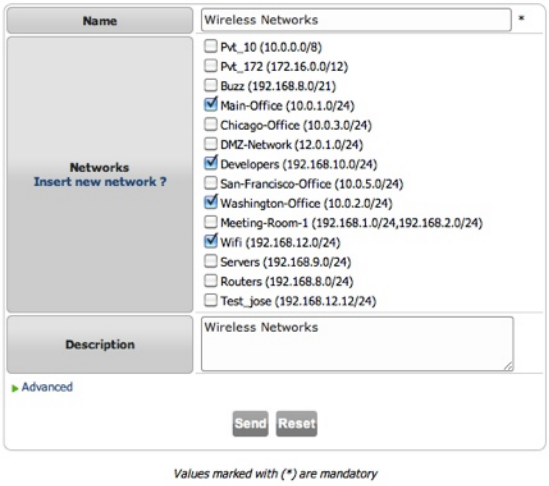
A Network Group in AlienVault has the following properties:

- **Name:** Label assigned to the Network.
- **Networks:** List of networks that are part of the network group:
- **Name:** Label assigned to the Network.
- **Description:** Short text describing the role of the networks that are part of the network group
- **Asset Value:** Value given to the network within the corporation
- **RRD Profile:** Profile to be used with the RRD Aberrant Behavior Plugin (Anomalies based on information provided by Ntop)
- **Threshold C:** Compromise threshold level
- **Threshold A:** Attack threshold level

Usage

New Network Group

To insert a new Network Group click on **New** in the upper left side.



Some of the properties of the Network Groups must meet special conditions:

- **Name:** Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used in the Hostname field.
- **Description:** Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used.
- **Threshold C:** Integer value
- **Threshold A:** Integer value

Modify a Network Group

To modify the properties of a Network Group select the Network Group in the grid using a single left click and then click on **Modify**.

When modifying a Network Group you will see the same properties that were described previously in the **Insert New Network Group** section.

Delete a Network Group

To delete a Network Group, click on the Network Group (Single left click) and then click on **Delete Selected.**

Ports

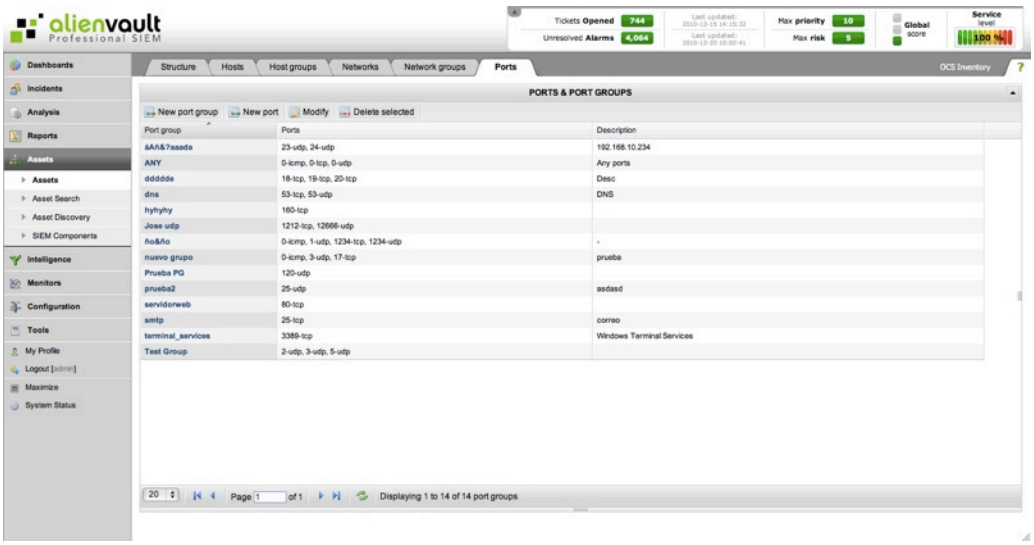
Assets -> Assets -> Ports

Description

When normalizing events in AlienVault, two of the mandatory fields that every event will have within AlienVault are Source Port and Destination Port. Whenever AlienVault is collecting an event with no source, no destination port or none of them the system will use 0 as port.

Ports are used in correlation, in the SIEM and Logger console and also it is possible to create Policy rules based on the destination port of the events.

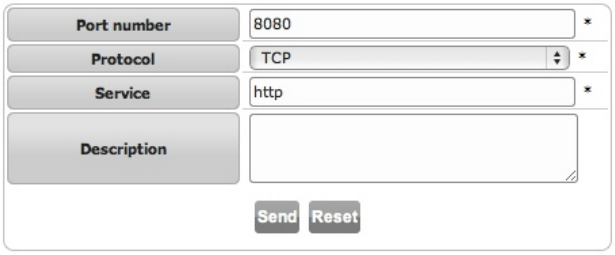
This page will allow inserting new Ports and creating Port Groups to be used in Policy rules or in correlation.



Usage

New Port

To insert a new port click on **New Port**.

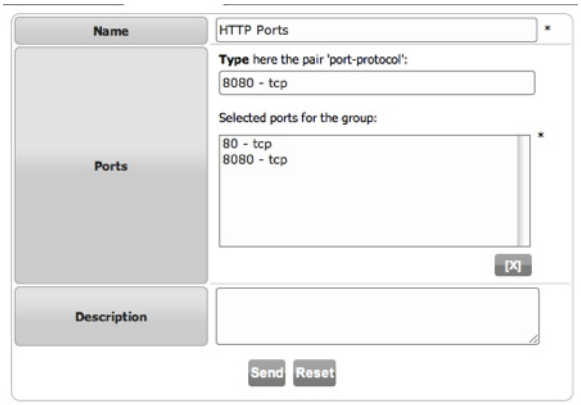


You will have to enter the following values:

- **Port number**: 16-bit unsigned integer, thus ranging from 0 to 65535.
- **Protocol:** TCP or UDP
- **Service:** Name of the service running on the port
- **Description:** Text describing the usage of this port

New Port Group

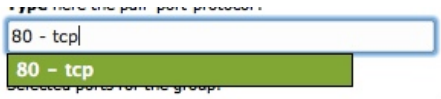
To insert a new port click on **New Port Group**



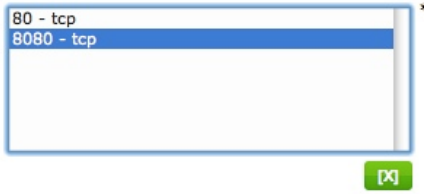
You will have to enter the following values:

- **Name**: Label given to the port group.
- **Ports:** List of ports part of the port group
- **Description:** Text describing the usage of this port group

To insert new ports in the port group simply write the number of the port and use the auto-completion feature to select, from the drop menu the port with its protocol that you would like to include in the Port Group.



To remove a Port from the port group select the port and click on **[X]**.



Modify a Port Group

To modify the properties of a Port Group select the Port Group in the grid using a single left click and then click on **Modify**.

Delete a Port Group

To delete a Port Group, click on the Port Group (Single left click) and then click on **Delete Selected.**

Assets Search

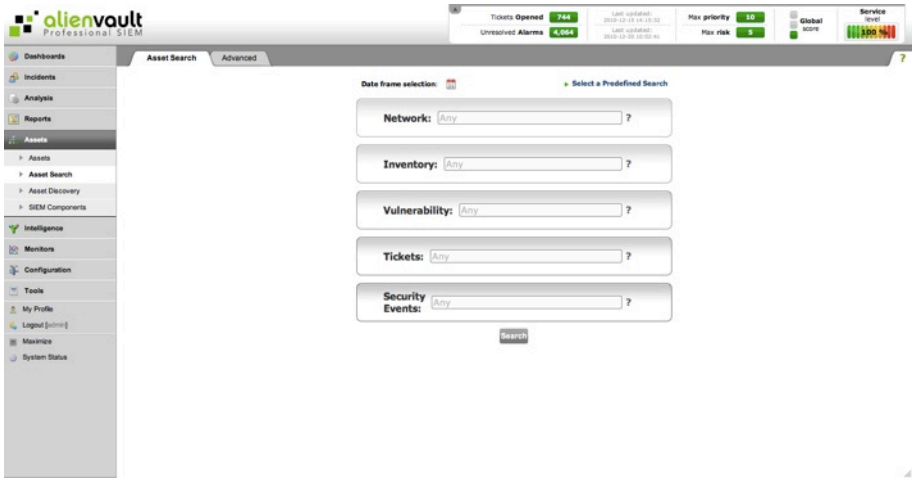
Simple

Assets -> Asset Search -> Simple

Description

Asset search lets you search for hosts that meet certain conditions. Some of these properties are the operating system or the services running on the hosts. You can also search hosts with a vulnerability or a specific event.

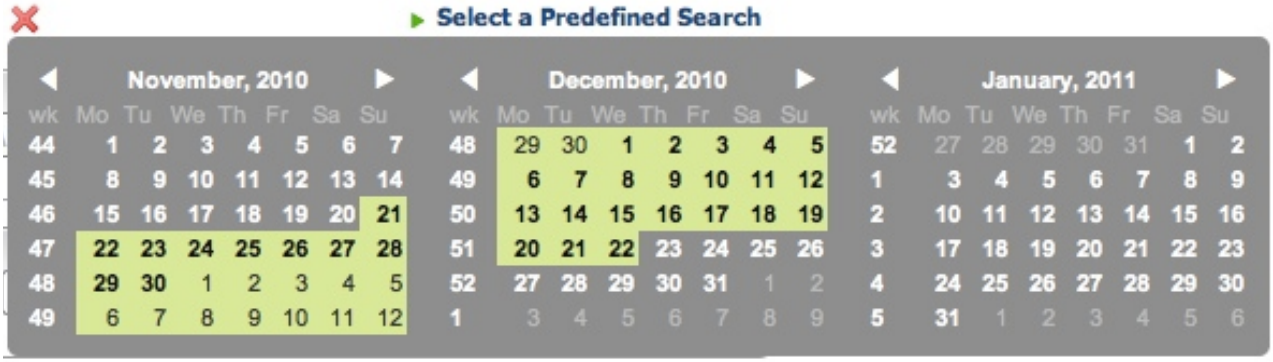
The search is performed on all the information that the system has in both the Logger (Filesystem storage) and the SIEM (SQL Storage).



Usage

Date Frame Selection

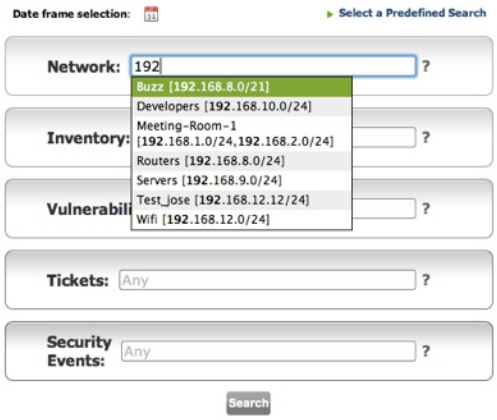
To select the time window on which the system will search for host click on the icon 



Dates in the yellow area will be included in the time window. Select your own and click on the red cross  to change the time window.

Simple Search

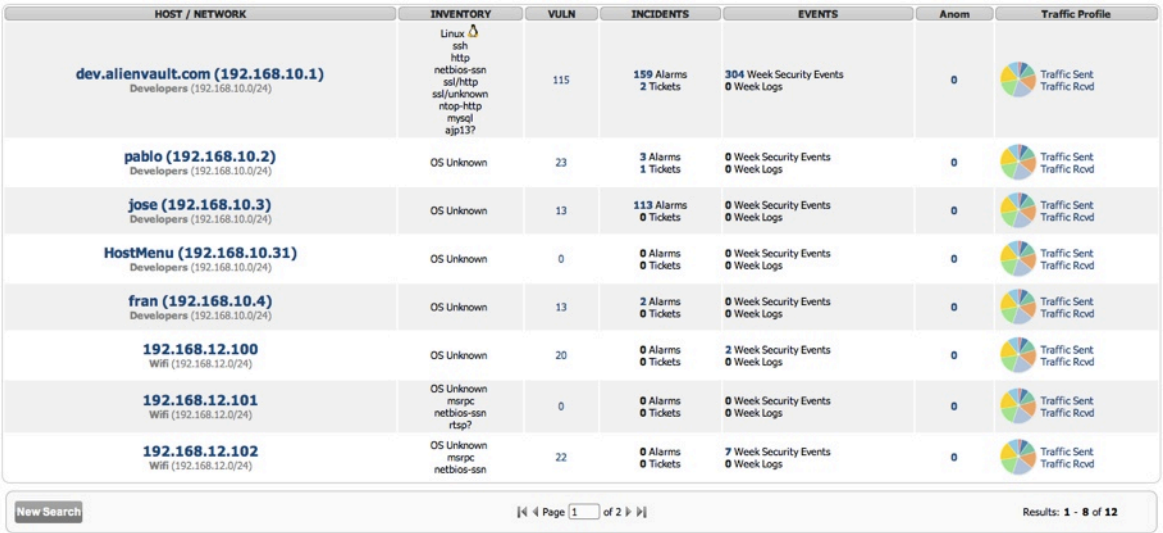
This form provides auto-completion in some of the fields. When writing you will get suggestions to speed up searches.



You can define your search criteria using the following fields:

- **Network:** Enter the name given to the Network (Assets -> Networks) or the network in CIDR format.
- **Inventory:** Enter an Operating System or a the name of a service (Assets -> Hosts)
- **Vulnerability:** Enter a text string that will be searched in the vulnerabilities found in the hosts (Analysis -> Vulnerabilities)
- **Tickets:** Enter a text string that will be searched in the ticketing system (Incidents -> Tickets)
- **Security Events:** Enter a text string that will be searched in the events stored in the SIEM (Analysis -> SIEM) and in the Logger system (Analysis -> Logger)

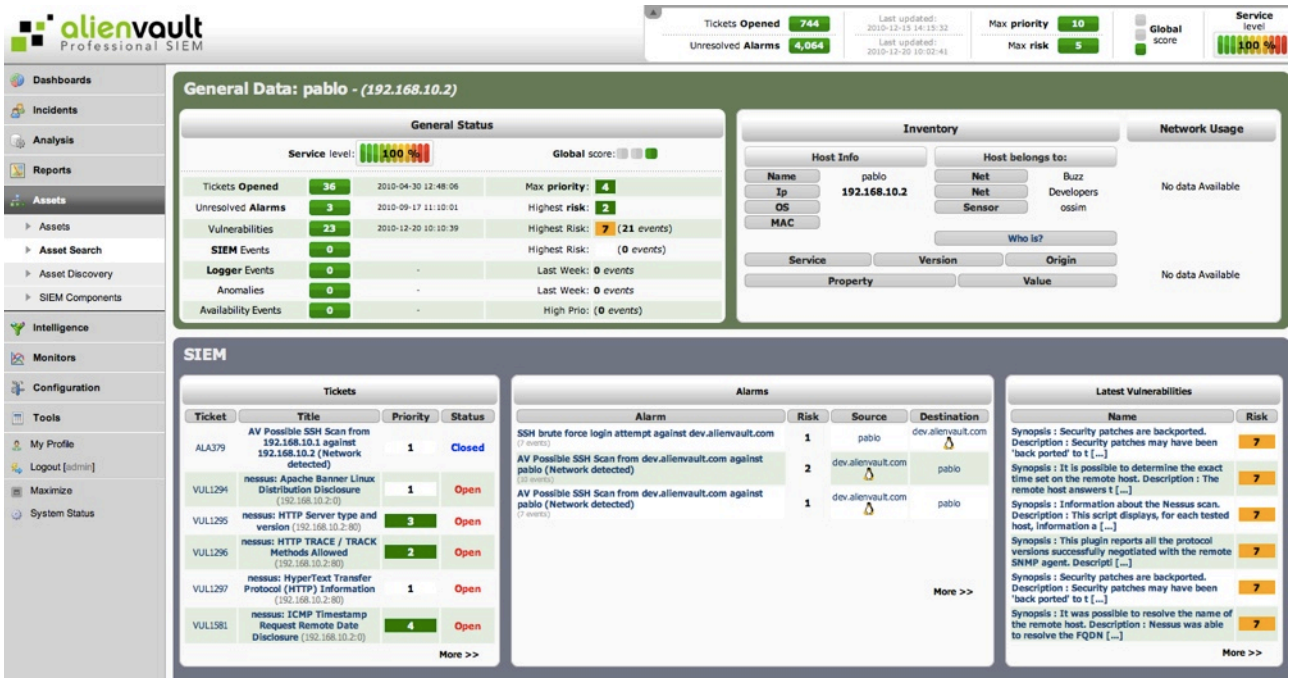
Once you have defined your search criteria click on **Search** and if one or more hosts are matching your search criteria you will get a list as the result of the search.



The search results are show in a table with the following columns

- **Host/Network:** Hostname, IP Address, name of the network the host belongs and network in CIDR format
- **Inventory:** Operating system and services running in the host
- **Vulnerabilities:** Number of vulnerabilities
- **Incidents:** Number of alarms and tickets in which this host is involved
- **Events:** Number of events in the SIEM and in the Logger from the host
- **Anomalies:** Number of anomalies generated by the host
- **Traffic Profile:** Link to Ntop graphs regarding the network traffic generated by the host

Clicking on the name of the Host will take you to the Host Report.



This Host Report includes all the information that the system has regarding a host such as:

- Events in SIEM and Logger
- Alarms
- Vulnerabilities
- Tickets
- Services
- Operating system
- Network Usage

Predefined Search

Using the Advanced Search functionality you can create your predefined searches. You can use this predefined searches clicking on **Predefined Searches**.

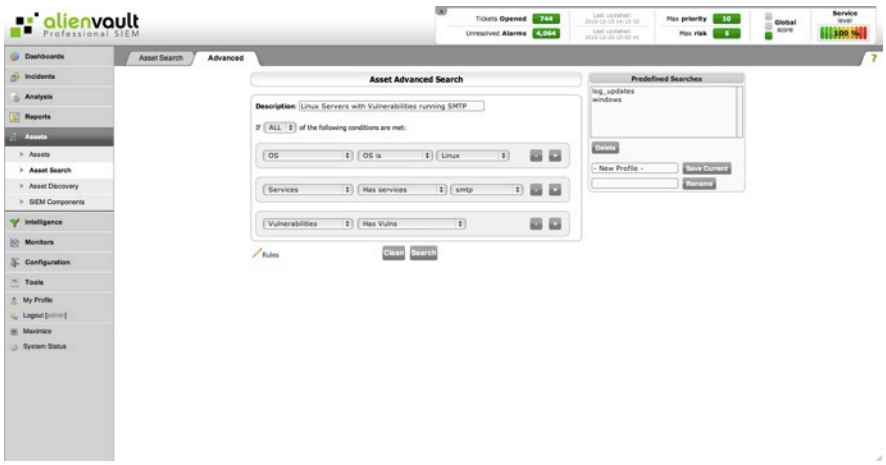
Advanced

Assets -> Asset Search -> Advanced

Description

Advanced Asset search allows more complex searches in all the data stored in AlienVault. This searches can be saved as predefined searches.

This allows a user with greater technical knowledge create searches that may be used by an operator with less knowledge.



Usage

Searches are created by combining search conditions. These conditions can be combined using an OR and AND logical operators. After inserting the description you will have to select if ALL conditions should be met (AND operator) or ANY condition should be met (OR operator).

Then select the condition or filter you would like to include from the drop-down list. Several conditions can be used:

- Operating System
- Services
- Mac Address
- Vulnerabilities
- SIEM Events
- META
- Alarms
- Ticket
- Asset
- Properties

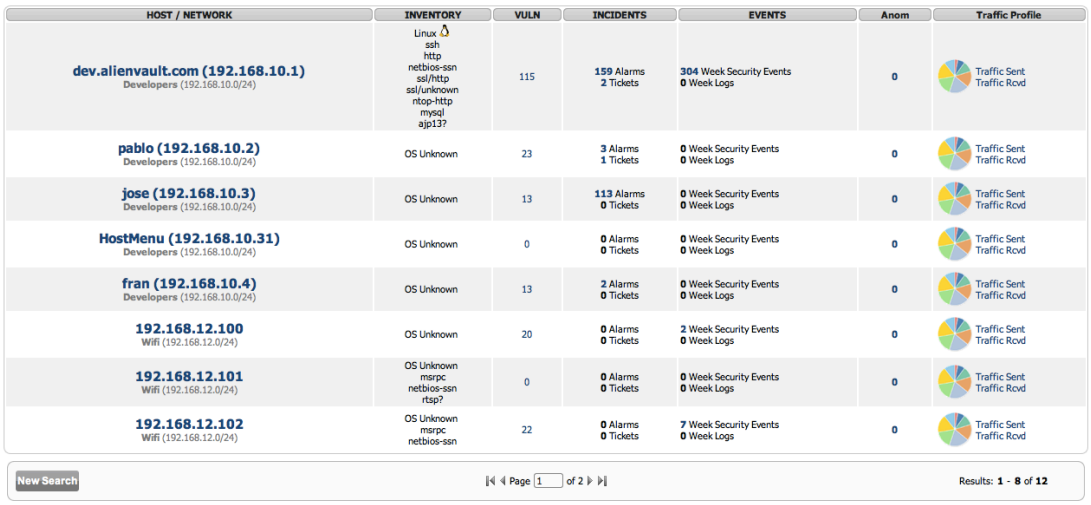
Each condition will have its own options, for example if we choose Vulnerabilities, we will get the following options:

- Has Vuln
- Vuln Contains
- Has Vulns
- Has no Vulns
- Vuln risk is greater than
- Vuln risk is greater than

Some of the conditions such as Has Vuln, will display a text box for you to write a text string that must be found in the vulnerabilities of a host. Some others, such as Has Vulns, indicate that the Host has Vulnerabilities, and no other option needs will be displayed.

You can combine as many conditions as you want. If you want to delete one of the conditions, click on the symbol **-** next to the condition. Once you have inserted all the conditions desired, click on **Search**. To clear all the search criteria click on **Clear**.

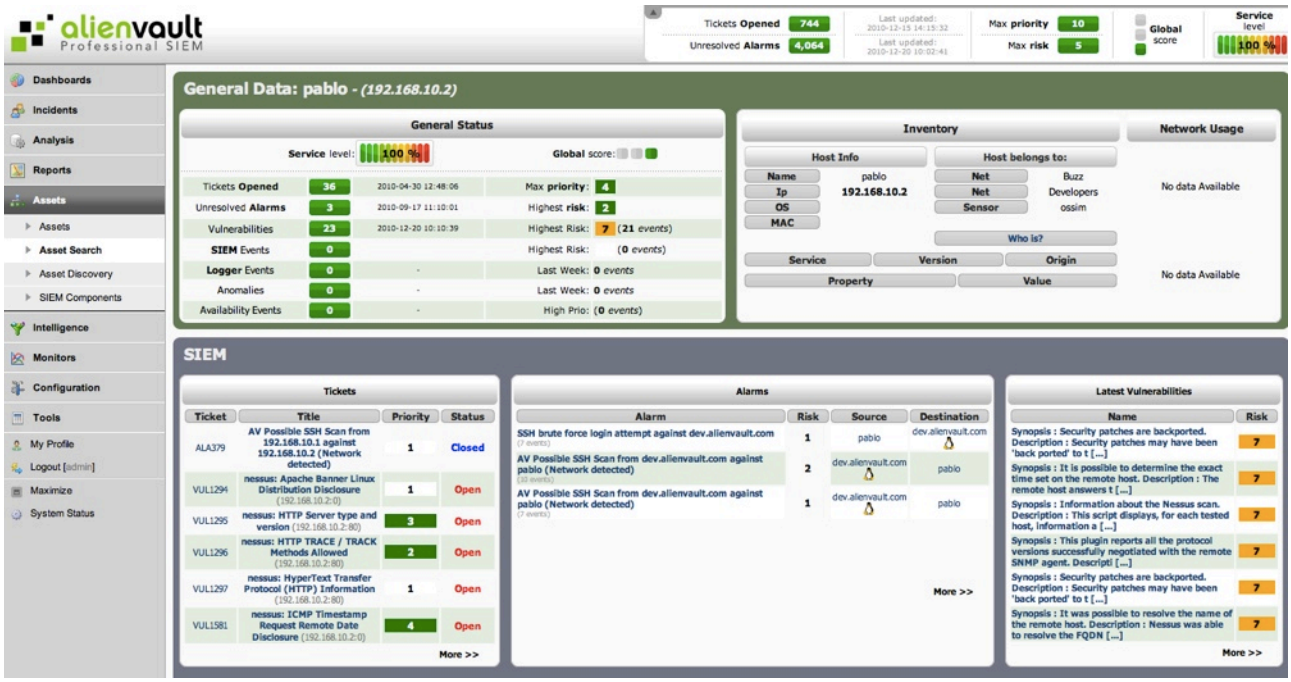
If one or more hosts are matching your search criteria you will get a list as the result of the search.



The search results are show in a table with the following columns

- **Host/Network:** Hostname, IP Address, name of the network the host belongs and network in CIDR format
- **Inventory:** Operating system and services running in the host
- **Vulnerabilities:** Number of vulnerabilities
- **Incidents:** Number of alarms and tickets in which this host is involved
- **Events:** Number of events in the SIEM and in the Logger from the host
- **Anomalies:** Number of anomalies generated by the host
- **Traffic Profile:** Link to Ntop graphs regarding the network traffic generated by the host

Clicking on the name of the Host will take you to the Host Report.



This Host Report includes all the information that the system has regarding a host such as:

- Events in SIEM and Logger
- Alarms
- Vulnerabilities
- Tickets
- Services
- Operating system
- Network Usage

Predefined Search

Once you have created all the search conditions you can save the search as a predefined search by clicking on **Save Current.**

To delete a Predefined Search select the search that you wish to delete and click on **Delete**.

SIEM Components

Sensors

Assets -> SIEM Components -> Sensors

Description

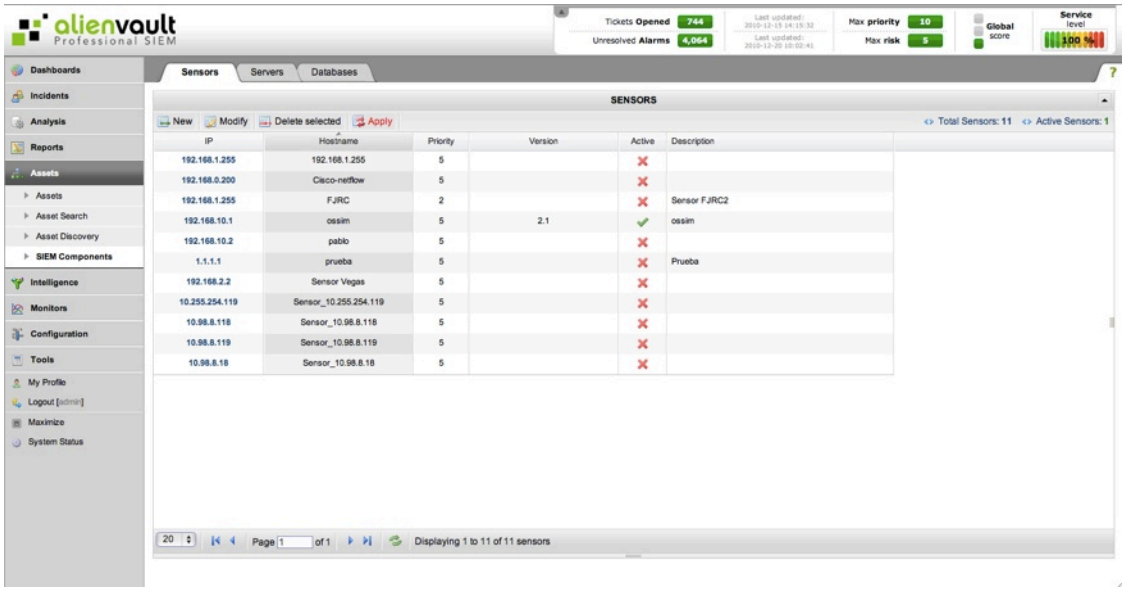
The AlienVault Sensor is the component in charge of collecting and normalizing the events generated by the Data Sources. Multiple Data Sources will feed events to the AlienVault Sensors such as Firewalls, Antivirus, AD, Database, and any other application or device that was used in the network before AlienVault was deployed. Some other Data Sources will be running in the same box that AlienVault does. We usually refer to this Data Sources as AlienVault Data Sources.

Snort, Ntop, Arpwatch, Pads, P0f, Fprobe and many others are AlienVault Data Sources. When you have a Sensor with no AlienVault Data Sources installed on it you will say that this sensor is a collector only. When we have a Sensor collecting events and generating events (Because the AlienVault Data Sources are running on it) we will say that this sensor is combining the Collector and the AlienVault Data Sources in the same box.

Sensor IP Addresses must be unique within the AlienVault deployment, because we may find a deployment in which we are monitoring the range of IP Addresses in two different locations. For this reason, hosts and networks will always be related to Sensors. And they should only be related to the sensors that are collecting events or traffic from the network. This will also be helpful when running the vulnerability scanning or the monitor requests during correlation, this will always be done from the sensors that are associated to the network or hosts and not from any other sensor in the AlienVault deployment.

An AlienVault deployment can have as many Sensors as required, the number of Sensors will basically depend on the number of networks that need to be monitored and in the geographical distribution of the corporation that will be monitored.

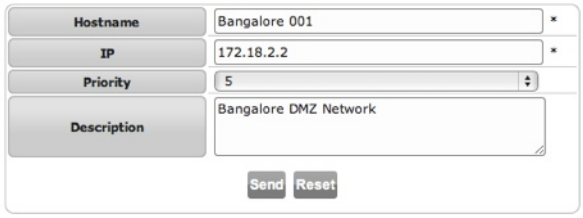
When a Sensor is sending events to the AlienVault Server and it has not been configured, you will see a message in the Web Interface and you will have to insert the New Sensor.



Usage

New Sensor

To insert a new Sensor click on **New** in the upper left side.

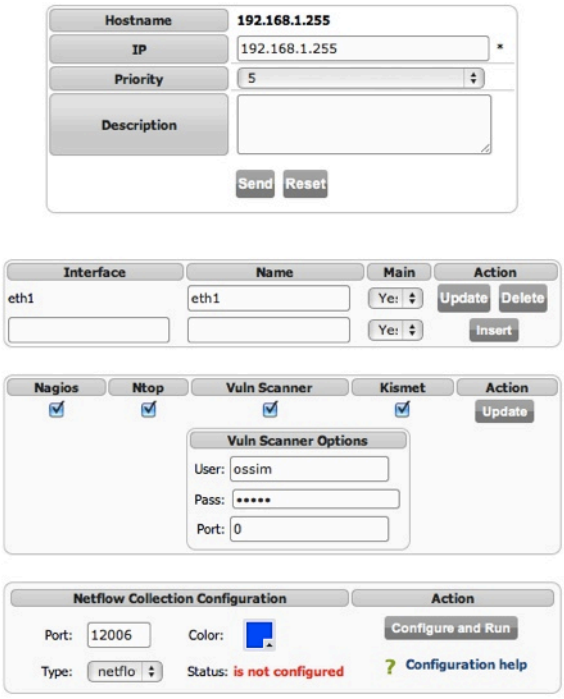


You will have to fill in the following properties:

- **Hostname**: Name of the Sensor. Alphanumeric characters and spaces. Some symbols such as "-" "_" can also be used in the Hostname field.
- **IP:** IP address of the Sensor in IPV4 format. In case the sensor has multiple IP Addresses you should enter the IP address that will be used to send events to the AlienVault Server.
- **Description**: Short Description of the Sensor (Location, Networks monitoring...). The description field is optional.

Modify a Sensor

To modify the properties of a Sensor select the Sensor in the grid using a single left click and then click on **Modify**.



Apart from the IP Address and the priority of the Sensor, some other properties can be modified.

The Web interface needs to know the interfaces (Network cards) running in promiscuous mode (Collecting traffic). This way you can switch between interfaces in Monitor -> Network -> Profile (Ntop Web Interface). You can also configure the main interface, which will be the default one when using the Ntop Web interface.

Enter the interface (Assigned by the Operating system E.g.: eth0, wlan0, en0, eth3...) and click on Insert. To delete an interface, click on Delete next to the interface that has to be deleted.

After that we can configure the tools that will be used from this Sensor. Notice that the tools need to be enabled also in AlienVault_setup.conf file in the Sensor.

If have Nagios installed and running in the Sensor you can enable Nagios, this way you will be able to switch between your different Nagios installations in the page Monitor -> Availability.

The default installation of the Sensor profile will also install Ntop. Enable Ntop to be able to see the Ntop Web interface of your Sensor from the AlienVault Web Interface.

If you enable the vulnerability scanner the Sensor will be used when running distributed vulnerability scans. It will ask you to write the user and password that has to be used to connect remotely to the vulnerability scanning server (OpenVas or Nessus). The default user will always be AlienVault, and the password will be the password stored in the file AlienVault_setup.conf (In the Sensor) in the variable pass.

If your sensor has also been configured to run Kismet to monitor your wireless networks, enable Kismet in the Sensor properties.

The last part of the Sensor properties refers to Flows collection. Fprobe is also installed and configured automatically to generate flows based on the network traffic the Sensor is collecting. The flows should be sent to the AlienVault box with running the Web Interface (Framework profile). Each Sensor or device generating Flows will use a different port to send the flows and a different color can be used to identify the flows depending on the device that has generated the flows.

Select the color that will identify the flows generated by the Sensor and click on Configure and Run. For more information on how to configure the Flows collection please refer to the section Network -> Traffic.

Delete a Sensor

To delete a Sensor, click on the Sensor (Single left click) and then click on **Delete Selected.**

Apply changes

Once you have inserted or modified the Sensors click on **Apply.** This will send a signal to the AlienVault Server to reload all the information regarding the Sensors that is used during correlation and in Policies.

Servers

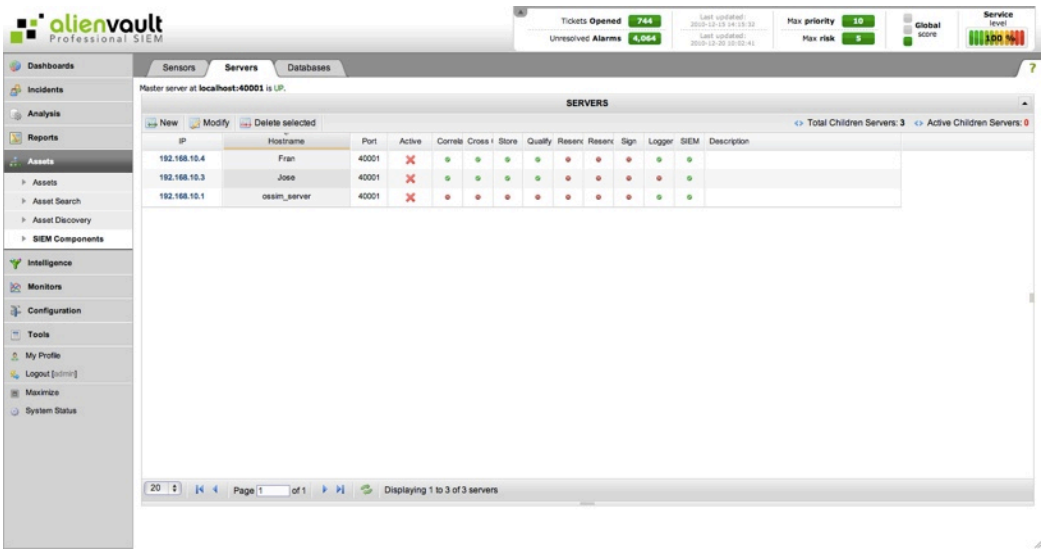
PRO ONLY

Assets -> SIEM Components -> Servers

Description

A simple AlienVault deployment will have a single server working as SIEM and Logger. Large and complex deployments can have multiple servers at multiple levels. Each server will always be configured to another server except the server on top, that will be called master server and that doesn't need another server on top.

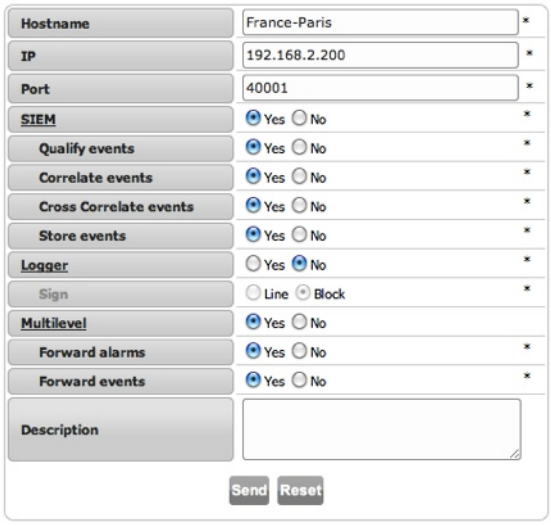
Multi-level deployment allows correlation at multiple servers and even storage at different levels. Using policies, you can define what type of events and alarms that will be exchanged with each server. Also what each server will do with each type of event. In this section you will basically need to insert all the AlienVault Servers that are part of your deployment, and the characteristics that will be enabled in each Server. If you have a single Server in your deployment you don't need to insert your server in this section.



Usage

New Server

To insert a new Server click on **New** in the upper left side.



You will have to fill in the following properties:

- **Hostname**: Name of the Server
- **IP**: IP address of the AlienVault Server (The IP address used by the Sensors to send events to the AlienVault Server)
- **Port**: AlienVault Server listening Port (By Default 40001)
- **SIEM**: Enable/Disable the SIEM functionality. If enabled the following properties can also be enabled or disabled:
  - **Qualify Events**: Risk calculation for the events (Intrinsic Risk and Aggregated Risk)
  - **Correlate Events**: Enable/Disable Logical correlation (Using correlation directives)
  - **Cross correlate Events**: Enable/Disable Cross Correlation
  - **Store Events**: SQL Storage
- **Logger**: Enable/Disable the Logger functionality. If enabled the following properties can also be enabled or disabled
  - **Sign**: Enable/Disable the digital signature for events stored in the Logger
- **Multilevel**: Enable/Disable the forwarding functionality. If enabled the following properties can also be enabled or disabled
  - **Forward alarms**: Enable/Disable the alarms forwarding to an upper server
  - **Forward events**: Enable/Disable the events forwarding to an upper server

These properties configure the default behavior of each server but they can be overridden using Policies.

Modify a Server

To modify the properties of a Server select the Server in the grid using a single left click and then click on **Modify**.

Delete a Server

To delete a Server select the Server in the grid using a single left click and then click on **Delete Selected**.

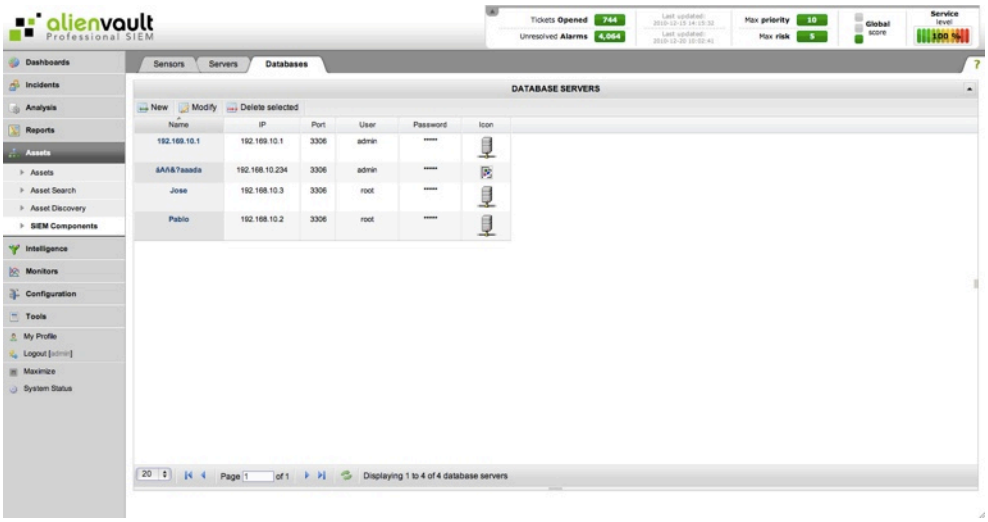
Databases

PRO ONLY

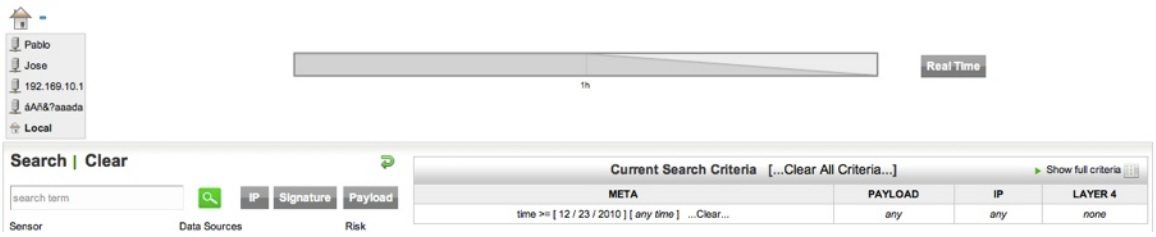
Assets -> SIEM Components -> Databases

Description

Multi-level deployments can have SQL Storage at different levels. Depending on how event and alarm forwarding has been configured, the Master Server may not receive all the events and alarms that have been generated and collected in the deployment.



When doing a forensic analysis the user may need to connect to another Database storing events in the deployment. For this reason all the databases should be configured in the main Web interface. If you do this and then you use the SIEM Forensic tool (Analysis -> SIEM -> SIEM) you will see this icon that will allow you to switch between the different databases in your deployment.

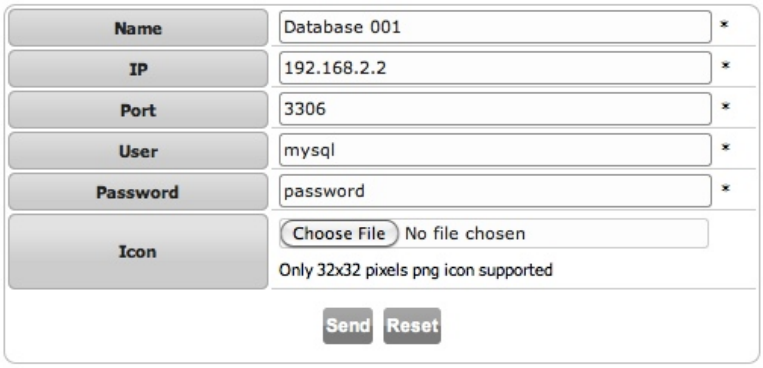


Only AlienVault databases should be configured in this section. In case your deployment is using a single database then you don't need to configure anything in this section.

Usage

New Database

To insert a new Database click on **New** in the upper left side.



You will have to fill in the following properties:

- **Name**: Name given to this database
- **IP**: IP address of the host running the Database. MySQL must be listening in that IP address (bind-address parameter in my.cnf)
- **Port**: MySQL listening Port (By Default 3306
- **User**: Username in the MySQL Server
- **Password**: Password for the username in the MySQL Server

It is possible to upload an icon that identifies this database in the drop-down menu in SIEM->Analysis

You may need to configure your MySQL Server to accept remote connection from the main AlienVault Web interface using the user you just wrote when inserting the properties of the new database.

Modify a Database

To modify the properties of a Database select the Database in the grid using a single left click and then click on **Modify**.

Delete a Database

To delete a Database select the Database in the grid using a single left click and then click on **Delete Selected**.

Intelligence

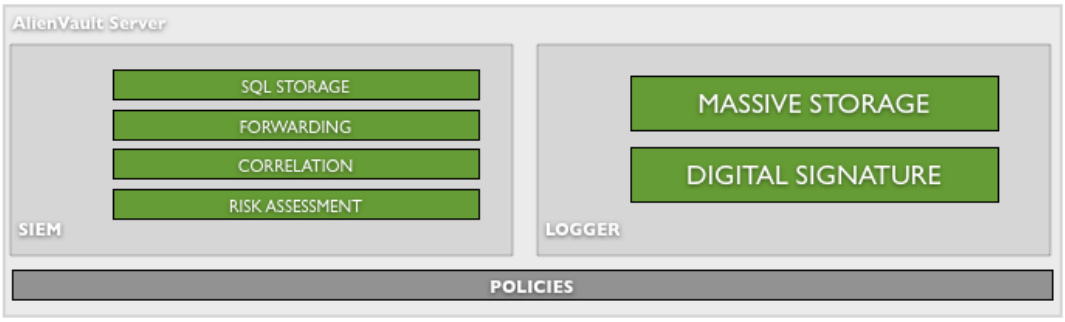
Policy & Actions

Policy

Intelligence -> Policy & Actions -> Policy

Description

Policy section allows you to configure how the system will process the events once they arrive to the AlienVault Server. All events will go through the following processes within the AlienVault Server:



By default the all the events arriving to the AlienVault Server are processed by both SIEM and Logger (Only when using the Unified SIEM).

In the case of SIEM the system provides extra intelligence and data-mining capabilities processing the events by performing the following tasks.

- **Risk assessment**: A risk is assigned to each event taking into account the type of event and the assets involved in the generation of the event.
- **Correlation**: Correlation is the process of Transforming Into Various data input to output new data element. Using correlation AlienVault can transform two or more input events into a more reliable output events. Events generated during the correlation process are re-injected back to the AlienVault Server and processed the same way as if these were being sent by one of the Sensors.
- **Forwarding**: The AlienVault Server may be configured to send events and alarms to an upper Server (Parent Server) in multi-level deployments.
- **SQL Storage:** Events processed by the SIEM are stored in a SQL Database (MySQL Database).

In the case of Logger, the system will sign the events to ensure integrity so that they can be used as evidence in trial.

When defining a policy is necessary to define the conditions that the events must comply in order to match one of the Policy rules.

Policy rules also define what features of the SIEM and Logger will be enabled to process the events matching the policy rules.

Policy rules are applied in descending order and when an event matches a rule, the system will stop processing that event, so that it will not be able to match any other policy rule defined subsequently. For this reason the generic policy rules should be always defined after the policy rules used to configure exceptions for certain events.

This page shows a series of tables, each table is a group of policies. These are the fields that are shown with each of the policy rule:

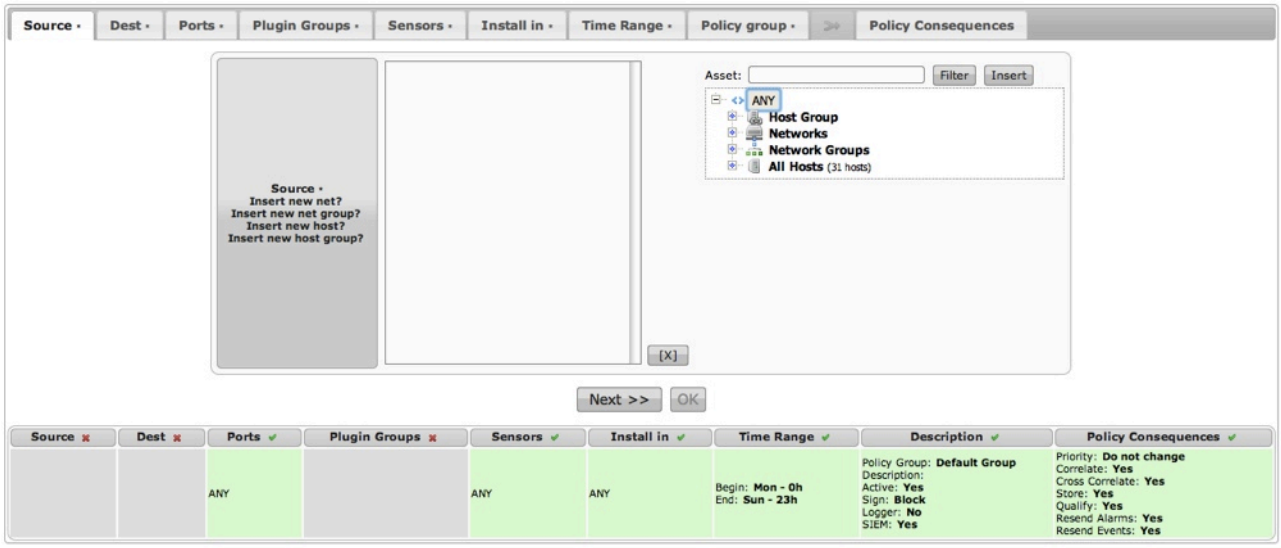
- **Status:** Policy Rule enabled:  / Policy Rule disabled 
- **Order:** Position in which this policy rule will be loaded
- **Priority:** Wether the priority of the events matching this policy rule has to be modified or not, and if modified, the value of the new priority (Only applies if SIEM is enabled)
- **Source:** Sources matching this policy rule (Hosts, Host Groups, Networks, Network Groups...)
- **Destination:** Destinations matching this policy rule (Hosts, Host Groups, Networks, Network Groups...)
- **Port Group:** Destination port of the events that will match this policy rule.
- **Plugin Group:** Group of event types that matching this policy rule.
- **Sensors:** Sensor or Sensors collecting the events matching this policy rule
- **Time Range:** Time period in which this policy rule will be enabled.
- **Targets:** Servers in which this policy rule will be installed (Multi-level deployments)
- **Correlate:** Enables / Disables logical correlation for the events matching this policy rule (Only applies if SIEM is enabled)
- **Cross Correlate:** Enables / Disables cross correlation for the events matching this policy rule (Only applies if SIEM is enabled)
- **Store:** Enables / Disables SQL Storage for the events matching this policy rule (Only applies if SIEM is enabled)
- **Qualify:** Enables / Disables risk calculation for the events matching this policy rule (Only applies if SIEM is enabled)
- **Resend Alarms:** Enables / Disables alarms forwarding to an upper server for the events matching this policy rule
- **Resend Events:** Enables / Disables events forwarding to an upper server for the events matching this policy rule
- **SIEM:** Enables / Disables SIEM for the events matching this policy rule
- **Logger:** Enables / Disables Logger for the events matching this policy rule
- **Sign:** Enables / Disables alarms forwarding to an upper server for the events matching this policy rule (Only applies if Logger is enabled)

Usage

New Policy Rule

To create a new Policy Rule click on **New** within the Policy Group in which you would like to include the new policy rule.

This will show the following screen.

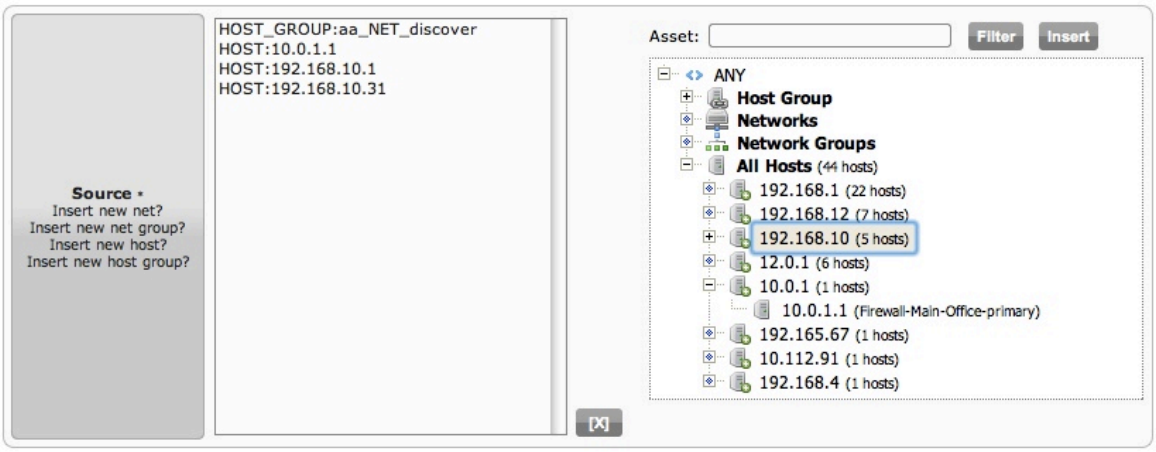


When creating a new policy rule you will have to define the conditions that have to be met for the events to match that policy rule as well as the consequences that the policy will have when the events are being processed by the AlienVault Server.

The following conditions have to be configured when creating a policy rule:

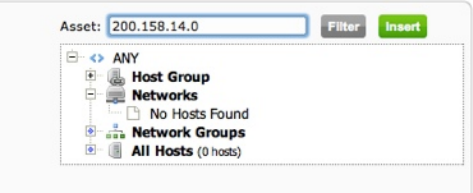
Source

Insert in the Source the Assets (Networks, Hosts, Host groups, Network Groups) that must appear in the Source IP field of the events matching this policy. By default the source will be set to ANY.



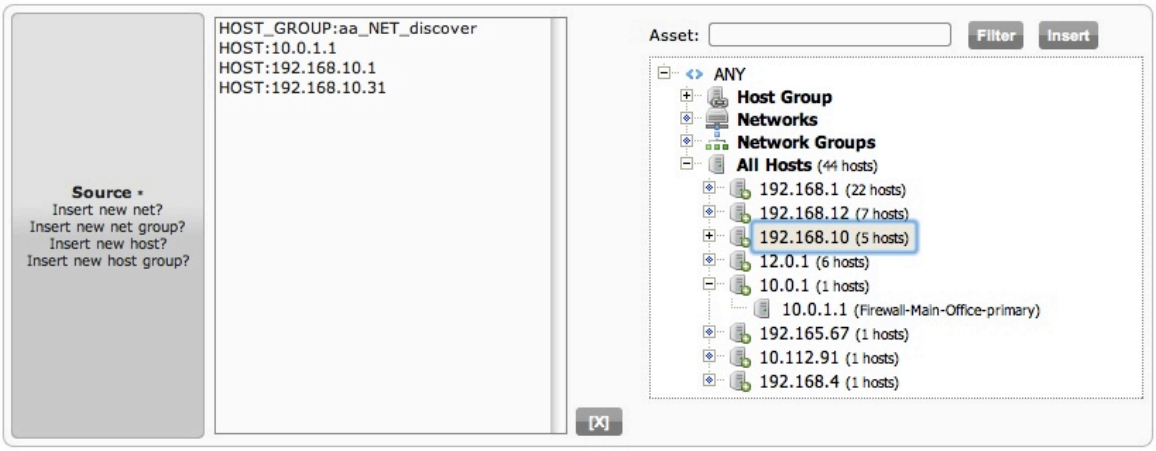
You can also filter the hosts shown in the tree writing a search string in the box above the tree and clicking on **Filter**.

If you want to create a Policy rule using IP addresses that do not belong to your inventory type the IP address in the box above the tree and click on **Insert**.



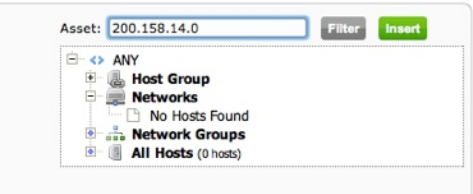
Dest (Destination)

Insert in Dest the Assets (Networks, Hosts, Host groups, Network Groups) that must appear in Destination IP field of the events matching this policy. By default the destination will be set to ANY.



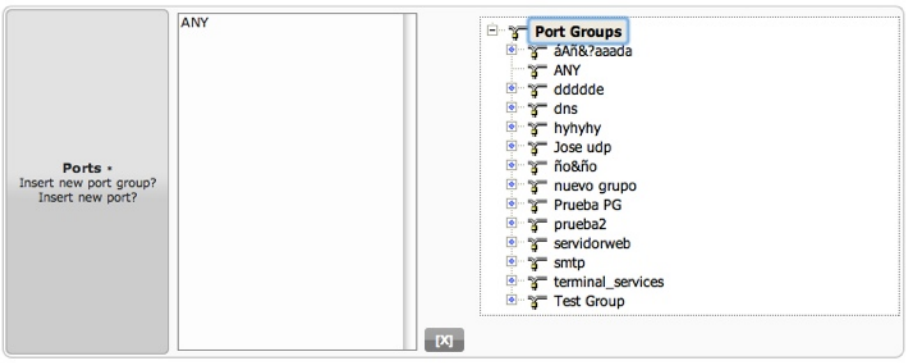
You can also filter the hosts shown in the tree writing a search string in the box above the tree and clicking on **Filter**.

If you want to create a Policy rule using IP addresses that do not belong to your inventory type the IP address in the box above the tree and click on **Insert**.



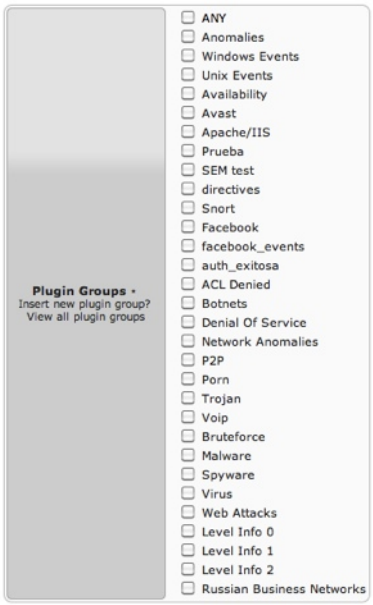
Ports

In ports you can configure the port that must appear as destination port in your events. By default this will be set to any. If you want to create a policy rule that only matches events having one or more destination ports, you create the Port Group first (Refer to the documentation of Assets -> Ports) and then select the Port Group in this Policy form.



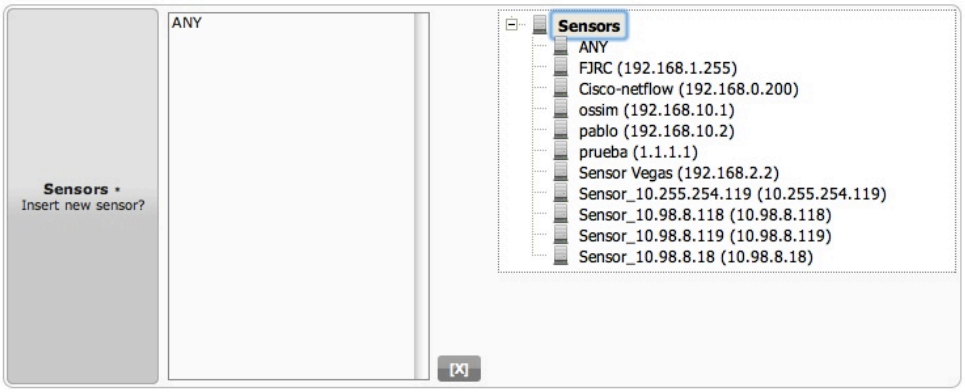
Plugin Group

In Plugin Group we need to select which type of events will be matching this Policy rule. By default this value will be set to ANY. This means that every event type will match this policy. To select only certain events you need to create a Plugin Group first. Please refer to the documentation of Plugin Groups (Configuration -> Collection -> Plugin Groups) to learn how to create Plugin Groups.



Sensors

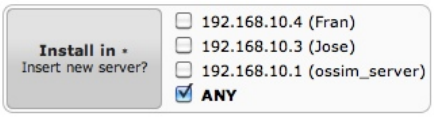
When the events are processed by the AlienVault Server, the Server knows the Sensor that was collecting the event. You can also create a Policy that works only for events collected by certain Sensors. By default the policy will match events coming from ANY sensor.



Install in

PRO ONLY

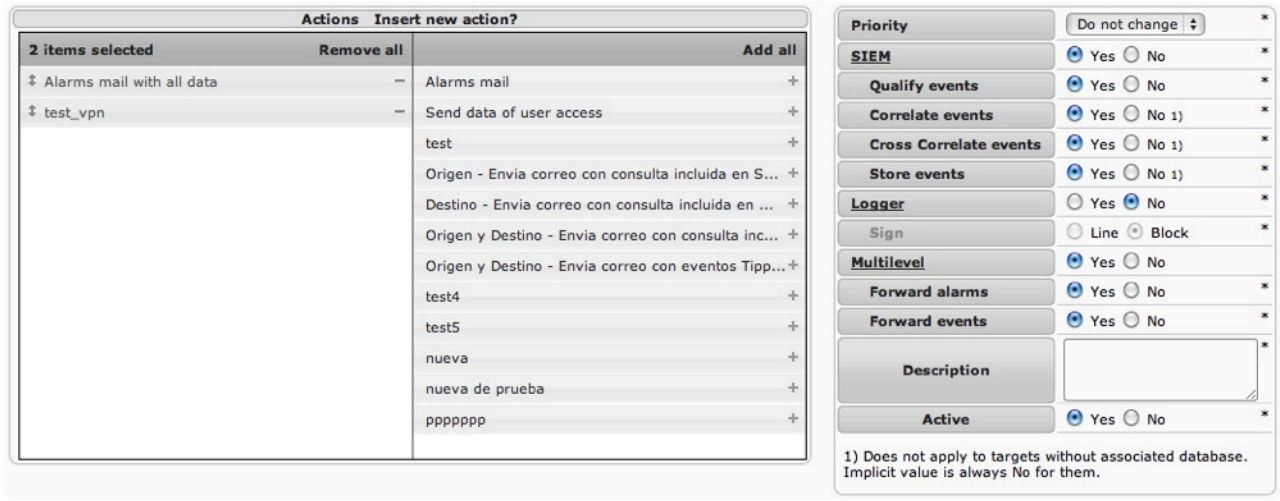
In multilevel deployments where multiple servers are deployed, you can configure a policy rule in your Master Server and install that policy in one of the children servers. By default policies will be installed on every Server.



Time Range

A policy can be enabled only at certain time during the week, for example, at night, or during the weekend.

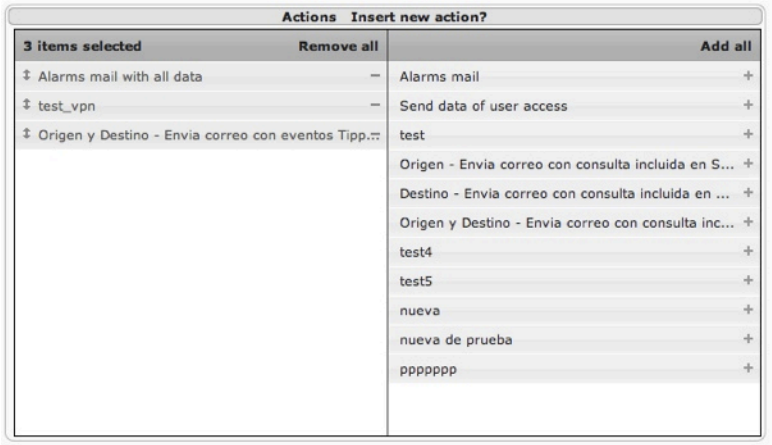
The consequences of the policy will be configured in the last tab called Policy Consequences:



In the left side, you will find the actions. Actions can be linked to policies, so whenever a Policy is matched the system can automatically launch an action to send an e-mail or run a Linux command. This allows creating firewall rules automatically, send SMS, shutdown a host remotely...

Actions are inserted in the tab Intelligence -> Policy & Actions -> Actions. Please refer to the documentation of that section to see how to insert new Actions.

Actions in the left side will be executed whenever an event matches the policy rule. You can just drag and drop actions from the right side to the left side, or click on **Add All** if you want to execute them all. If you want to stop executing one of the actions just drag and drop from the left side to the right side or click on **Remove all** to stop executing all the actions that were enabled.

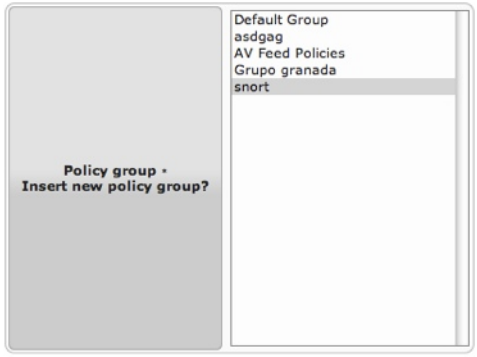


These are the rest of the consequences that can be used to create exceptions for certain events:

- **Priority**: Modifies the priority of the events overriding the default priority for that type of event (This affects Risk calculation)
- **SIEM**: Enable/Disable the SIEM functionality. If enabled the following properties can also be enabled or disabled:
  - **Qualify Events**: Risk calculation for the events (Intrinsic Risk and Aggregated Risk)
  - **Correlate Events**: Enable/Disable Logical correlation (Using correlation directives)
  - **Cross correlate Events**: Enable/Disable Cross Correlation
  - **Store Events**: SQL Storage
- **Logger**: Enable/Disable the Logger functionality. If enabled the following properties can also be enabled or disabled
  - **Sign**: Enable/Disable the digital signature for events in the Logger
- **Multilevel**: Enable/Disable the forwarding functionality. If enabled the following properties can also be enabled or disabled
  - **Forward alarms**: Enable/Disable the alarms forwarding to an upper server
  - **Forward events**: Enable/Disable the events forwarding to an upper server

The **active** field enables or disables the policy, this way you can create some policies to be enabled later.

Once a lot of policy rules have been defined it may be interesting to create Policy Groups to keep the policy rules well organized. You can select the Policy Group in which you want to include your new policy in the Policy Group tab. You can also move it to a different group later.



When creating or editing a policy rule you will always see a table in the bottom showing all conditions and consequences that have been configured in the policy rule:

Source	Dest	Ports	Plugin Groups	Sensors	Install in	Time Range	Description	Policy Consequences
HOST:192.168.1.99	HOST:192.168.1.98	ANY	Prueba	ANY	ANY	Begin: **Mon - 0h** End: **Sun - 23h**	Policy Group: **snort** Description: *s* Active: **Yes** Sign: **Block** Logger: **No** SIEM: **Yes**	Priority: **Do not change** Correlate: **Yes** Cross Correlate: **Yes** Store: **Yes** Qualify: **Yes** Resend Alarms: **No** Resend Events: **No**

Edit Policy Rule

To edit a Policy rule select the Policy rule in the grid using a single left click and then click on **Modify**.

Enable / Disable Policy rules

To enable or disable a Policy rule select the Policy rule in the grid using a single left click and then click on **Enable/Disable policy**.

Delete a Policy Rule

To delete a Policy rule select the Policy rule in the grid using a single left click and then click on **Delete Selected**.

Duplicate a Policy Rule

To duplicate a Policy rule select the Policy rule in the grid using a single left click and then click on **Duplicate Selected**.

Now you will have the possibility of modifying the conditions and consequences as if you were inserting a new policy rule.

Change Policy Rules Order

The order in which the policy rules will be loaded in the AlienVault Server is very important. For this reason you may need to change the order of the policy rules. To do this you can drag and drop policies. Just click on the policy you want to prioritize and move it upwards.

You can also switch Policy rules between different policy groups.

Actions

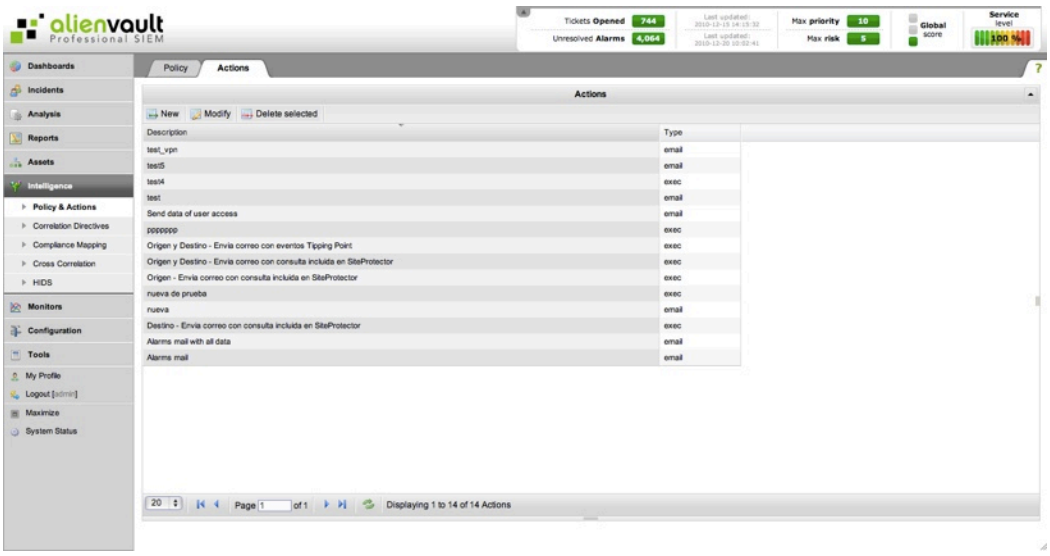
Intelligence -> Policy & Actions -> Actions

Description

The Actions page allows the user to define responses to attacks or problems happening in the network. Actions are related to policy rules, so that when a policy is matched all the actions related to that policy are executed.

AlienVault supports three types of actions, sending an e-mail, running a Linux command, or opening a ticket in the AlienVault Ticketing System (Incidents -> Tickets).

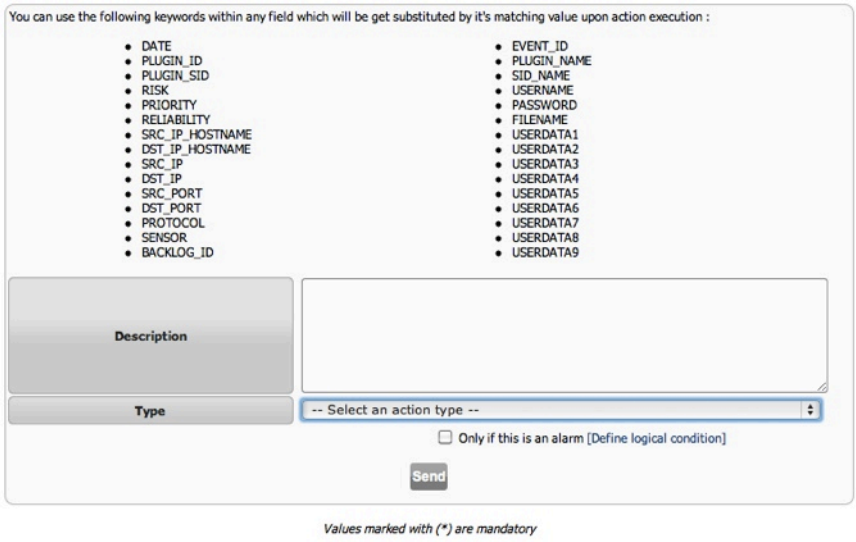
Some keywords can be used to create the actions so that these keywords are replaced by some properties of the event or events that matched that policy.



Usage

New action

To insert a new action click on **New** in the upper left side.



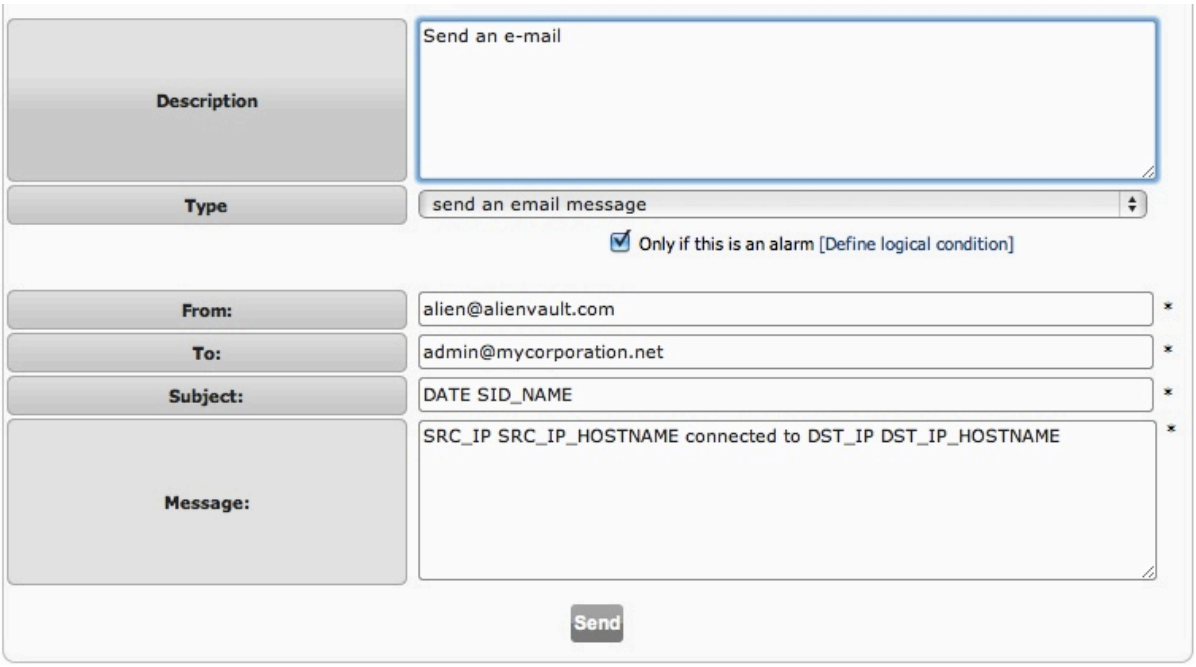
Write a short description explaining what this action does and select they type of action that you want to configure

- Send an E-mail
- Run a command
- Open a Ticket

This actions will always be executed in the AlienVault box running the Web interface profile (Framework).

When defining an action you can use the following keywords. These keywords will take the value of the variable referred in the events matching the Policy rule.

- DATE
- PLUGIN_ID
- PLUGIN_SID
- RISK
- PRIORITY
- RELIABILITY
- SRC_IP_HOSTNAME
- DST_IP_HOSTNAME
- SRC_IP
- DST_IP
- SRC_PORT
- DST_PORT
- PROTOCOL
- SENSOR
- BACKLOG_ID
- EVENT_ID
- PLUGIN_NAME
- SID_NAME
- USERNAME
- PASSWORD
- FILENAME
- USERDATA1
- USERDATA2
- USERDATA3
- USERDATA4
- USERDATA5
- USERDATA6
- USERDATA7
- USERDATA8
- USERDATA9



When creating the action you can also configure the action to be executed only if the events matching the policy have become alarms (RIsk >= 1).

Modify an action

To modify an action select the action in the grid using a single left click and then click on **Modify**.

Delete an action

To delete an action select the action in the grid using a single left click and then click on **Delete Selected**.

Correlation Directives

Directives

Intelligence -> Correlation Directives -> Directives

Description

Correlation

Event correlation is a technique for making sense of a large number of events and pinpointing the few events that are really important in that mass of information.

AlienVault can correlate events generated by any tool or device regardless of the type and format of event. The events will be normalized before the correlation takes place.

In AlienVault, logical correlation is implemented using Correlation Directives or Correlation rules. The correlation directives define different conditions that will be met by the incoming events. Whenever a condition has met the system will generate new events that can even meet some other conditions in a different correlation directive.

Server

Correlation in AlienVault takes places in the AlienVault Server. The AlienVault Collectors will collect events from the different devices or applications (Detectors). Once the events have been normalized they will be sent to the AlienVault Server.

Correlation happens whenever the SIEM functionality is enabled and if the correlation has not been disabled when defining policies to handle incoming events.

Correlation Directives

Correlation directives are written using XML syntax. By default, AlienVault includes over 200 directives of correlation. The Professional Feed provides greater coverage against attacks and network problems with more than 600 directives.

When a new plugin has been devolved, the user to integrate a device or tool is to create new correlation rules Correlation directives are stored in .xml files in the following directory:

/etc/AlienVault/server/

Correlation directives are stored in different files according to the category they belong to. The category will be assigned depending on the type of behavior that is being detected by the directive.

Correlation directives created by the users will always have to be stored in the following file:

/etc/AlienVault/server/user.xml

This will prevent loosing directives after an upgrade, since this is the only file that will not be updated automatically.

Whenever new tools and devices are integrated in AlienVault, new directives will not be created automatically. The user will have to create their own directives to detect complex behaviors and patterns in the new events. If you share your new plugins with the community then you will get more chances of having more correlation directives as the AlienVault team and the community will create some that will be useful in your environment.

Source of information

The correlation directives will create patterns for incoming events. Two different types of events will feed the correlation engine:

Detector

They offer events (Snort, Firewalls, Antivirus, Web servers, OS events..). Detector plugins are constantly sending information to the Correlation Engine. Once the event has been generated by the collector, the AlienVault Collector will collect and normalize the event before sending it to the Correlation Engine.

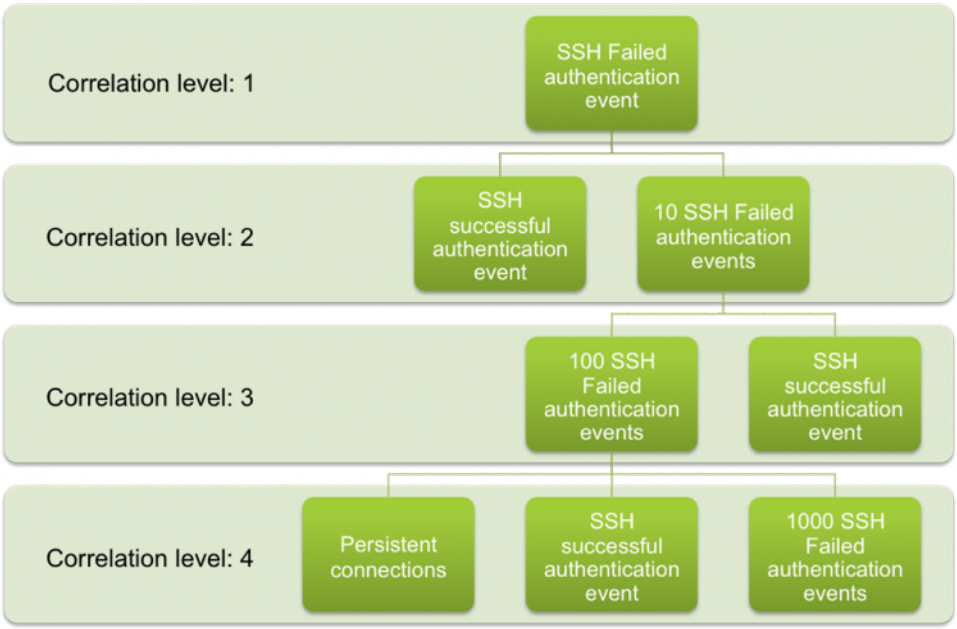
Monitor

They offer indicators (Ntop, Tcptrack, Nmap, Webs, Compromise & Attack…). Monitor plugins offer information to the correlation engine in request by the AlienVault Server during the correlation process.

Correlation rules

Each correlation directive consists of at least one correlation rule. Each correlation level contains as many rules as necessary, except the first correlation level that will always have a unique correlation rule.

The correlation rules define a set of conditions to be met for the events getting into the correlation directive.



Usage

New Correlation Directive

New correlation rule

Correlation Directives are created using a wizard that simplifies the process of writing a directive. To create a new correlation directive click on **Add Directive.**

Set the name of the directive, This is the name that will take all the events generated within this directive. You can use the following variable to be replaced by the value of the variable when the alarms are displayed in the Web console (Incidents → Alarms): SRC_IP, DST_IP, SRC_PORT and DST_PORT.

After setting the name click on **Next**.

Choose the category for this directive. The default category is User.

Choose the Priority of the directive. Priority will be numerical value from 0 up to 5. All events generated within the same directive will have the same directive but they may have a different reliability as it will depend on the correlation level in which the event has been generated.

If you set the priority to 0, events generated within the directive will never become an alarm. If you set a high priority value, the directive may generate alarms after grouping just a few events.

Now its time to set the conditions for the first rule in the correlation directive.

All events will try to match the first level of every enabled correlation directive once they arrive to the AlienVault Server. This behavior can be modifying defining a policy in (Intelligence → Policy & Actions).

- The first rule of a directive will have special conditions:
- It will always be a detector rule. Monitor rules can not be used in the first level of directives.
- It will wait for a single occurrence of an event
- It will have no time out. The condition of the first level will last as long as the server is running and the directive enabled
- The event will only be generated for the first directive rule whenever the directive has only one correlation level

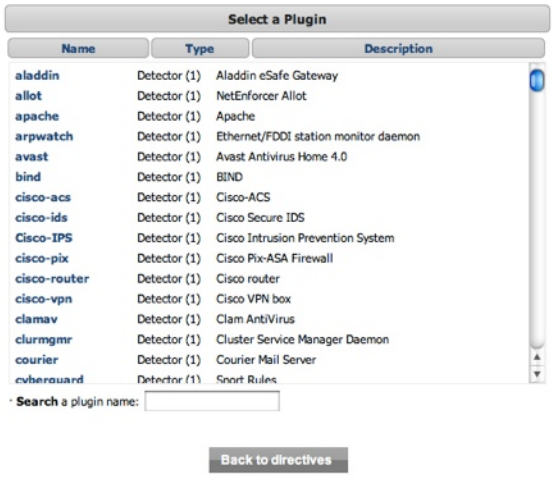
In the directive we are creating the correlation will start with any event coming from the SSH Server that refers to an authentication failed attempt. We should always try to cover all possible variants of an attack, in a SSH brute force attack we will find the following events:

- Failed Password
- User blocked
- Root login not allowed
- Illegal user
- User does not exist
- … and much more

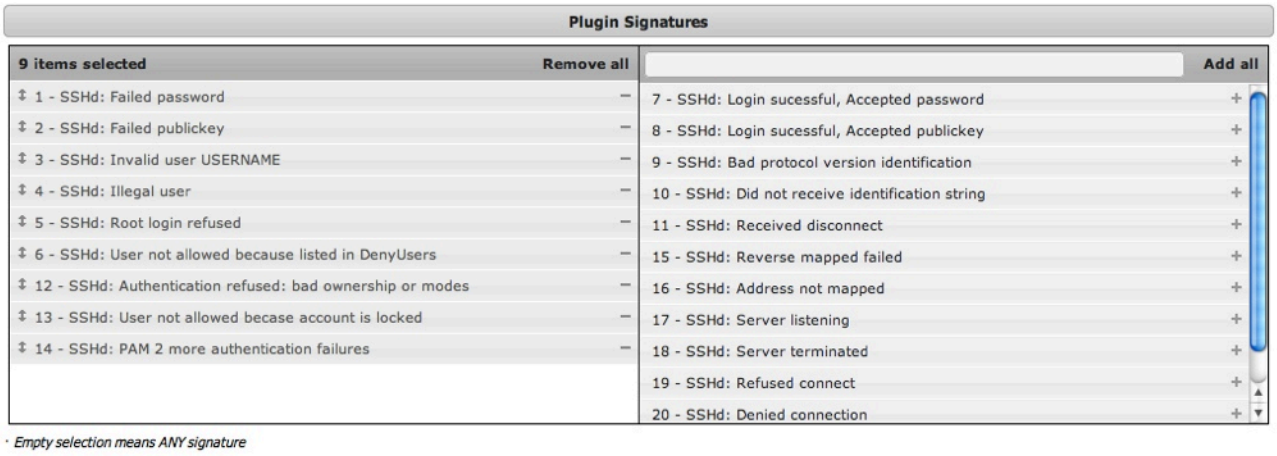
So when writing a correlation rule we should always think about all possible events that may be interesting for our new correlation rule. You can take a look to all events that can be generated by each plugin in the following section: Configuration → Collection

Each rule will always wait for events with the same Plugin ID. In this case we will be waiting for events with the Plugin ID 4003, and the following plugin SID which correspond to the type of events we get when we are suffering a brute force attack against one of our SSH Servers.

Select the Plugin from the list.

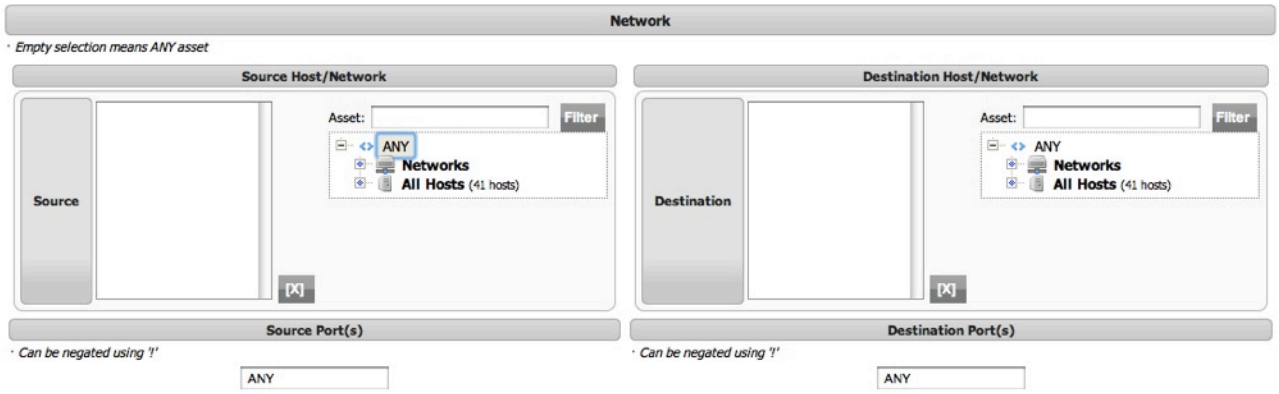


Now select the event types (Plugin SID's within this Plugin ID) that will match the first correlation rule. Event types in the left side are events that have already been added to the correlation rule. Events in the right side can be added to the correlation rule using drag and drop, by moving them to the left side. Event types can also be added to the correlation rule by clicking on +. To remove an event from the correlation rule click on - next to the event type that you wish to delete or click on **Remove all** to delete all event types from the correlation rule. In the top of the right column you can also search a text string and then click on **Add all** to include all events matching the search criteria in the correlation rule.



If you have no events in the left side, all events arriving to the correlation engine using the Plugin ID selected in the previous step will match the correlation rule. Once you have chosen the event types for this correlation rule, click on Next.

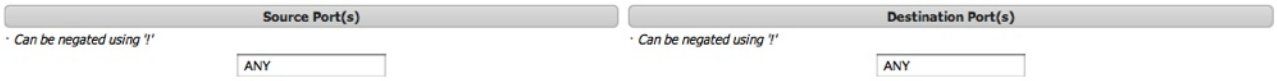
In this step, you have to define the sources and destination that can fulfill the conditions of the correlation rule. By default, any source and destination (internal or external) will meet the condition.



To define your own your own condition, use the trees displayed on the screen. The tree on the left is used for the source and the tree of the right is used for the destination. You can select multiple hosts or Networks. To select a host or a Network, simply click on the name of the host or network displayed in the tree.

To remove a host or network from your selection, click on the host or network that you wish to delete and then click on [X].

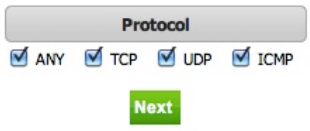
In this screen you can also define the source and destination ports of the events that will match the correlation rule. By default, any port will match the conditions defined by the correlation rule.



Insert as many port numbers for the source port and destination ports as you need. Ports must be in numerical format and separated by comma (No spaces). You can also use ANY as a keyword, and then negate some ports using [!]. E.g.: ANY,!80 means port except port 80.

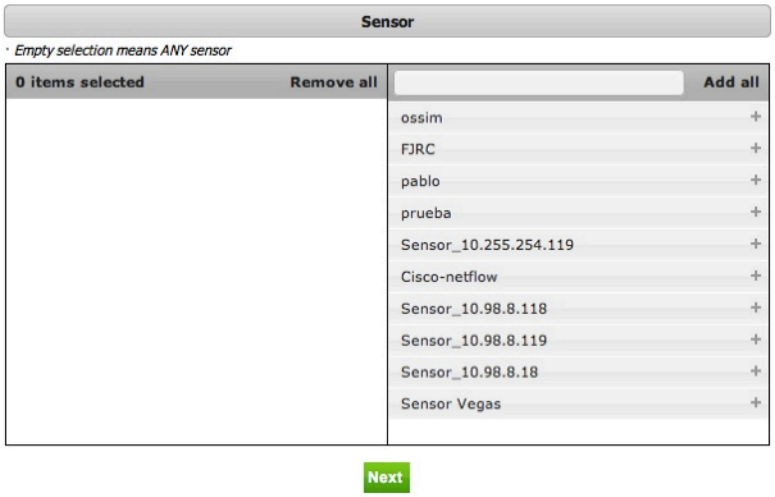
Once you configure both the conditions for the origin and destination, click on **Next**.

Some events (NIDS, Firewall ...) have a field indicating the network protocol that was being used at the time that the event was generated. This condition can be used in the correlation rule, so that the directive only works when the event has a particular protocol.



Click **Next** after setting the protocol condition. By default, any protocol will match the correlation rule conditions. A correlation rule can be configured to work only with the events collected by certain AlienVault sensors. By default, a correlation rule will work with events collected by every single AlienVault Sensor.

Sensors listed in the left side are Sensors that will enable the correlation rule (For events matching the rest of the conditions). Sensors in the right side can be added to the correlation rule using drag and drop, by moving them to the left side. Sensors can also be added to the correlation rule by clicking on +. To remove a sensor from the correlation rule click on - next to the sensor that you wish to delete or click on **Remove all** to delete all sensors from the correlation rule. In the top of the right column, you can also search a text string and then click on **Add all** to include all sensors matching the search criteria in the correlation rule.



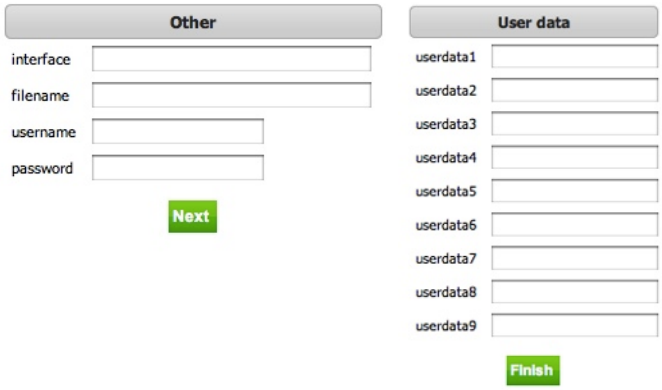
Whenever the condition established by the correlation rule is matched, a new event will be generated with a new reliability value. This event will be re-injected to the Correlation Server as if it came from another AlienVault Sensor. This event will have the priority value previously assigned as a global priority of the correlation directive, the reliability value defined in the correlation rule, and the asset value of the hosts matching the conditions of the correlation rule (In case they have a different asset value the highest one will be used).

The risk of the event will be calculated using the following formula:

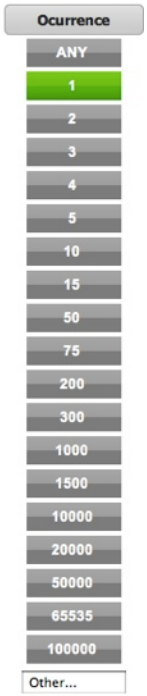
RISK = (Asset Value*Priority*Reliability)/2

Events that arrive at the correlation server can have assigned values in special fields (username, filename, password, userdata1, userdata2 ...). In this step you can define the value that should have these fields in order to correlate this rule successfully.

You can assign more than one value for each of the fields, separated by commas.

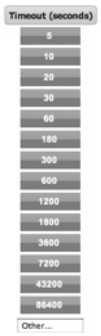


The number of occurrences determines how many events (meeting the conditions of the rule) must reach the correlation engine in order to correlate the rule successfully. Choose one of the predefined values or enter a custom value occurrences.



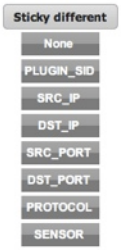
The timeout value determines how long the correlation server should wait (in seconds) before the correlation of the rule expires.

Select one of the default timeout values or enter a custom value. Timeout is a numerical value (In seconds)



In some cases it may be interesting to force a field to have a different value in each occurrence (Worms, Port scans ...). To make all the occurrences have a different value in one of the fields select the field from the list.

Eg: sticky_different = "dst_port"(All the events matching the rule Must Have A Different destination port (Port scanning detection))

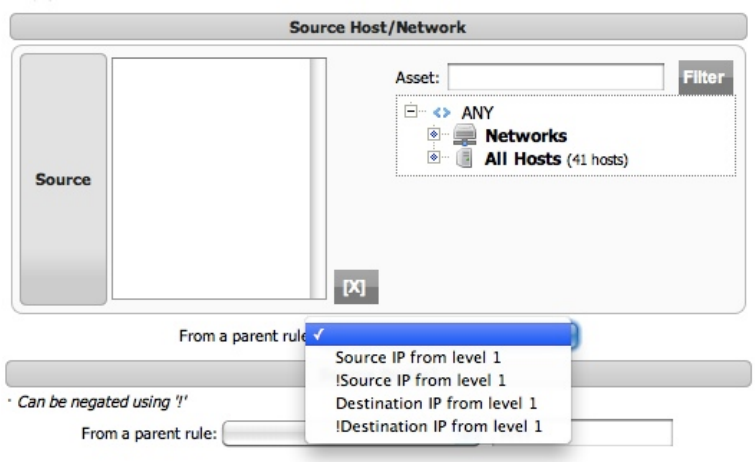


When editing rules (Rules other than the first correlation level) we can force some fields to have the same value that came in the events that matched the previous correlation levels. This can be done in the following fields of the correlation rule:

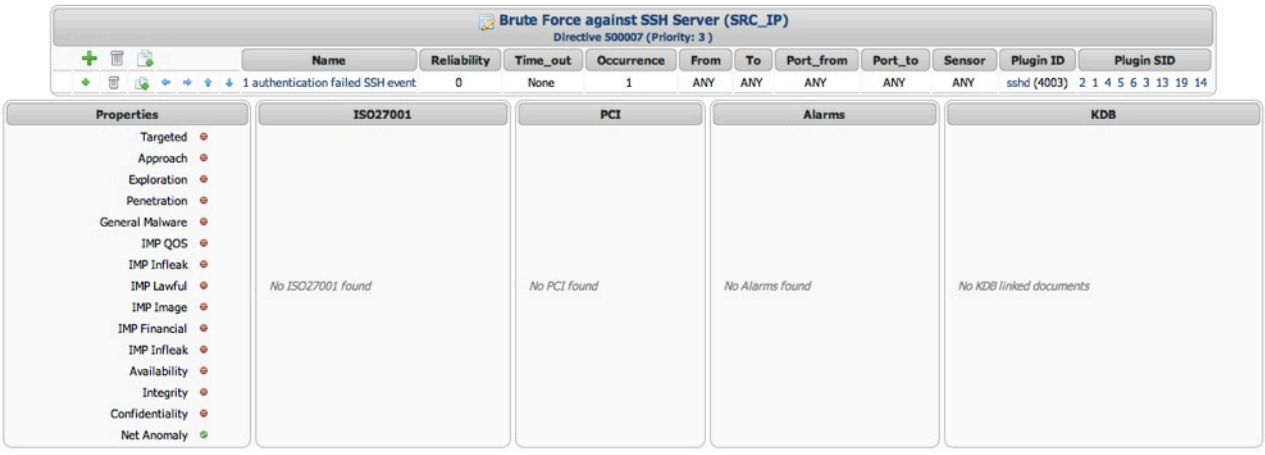
- plugin_id
- plugin_sid
- Source
- Destination
- Source Port
- Destination Port
- And all special fields (username, password, filename, userdata1-9)

When editing rules that are not at first correlation level, the wizard will show some drop boxes that let use the value of a field that came previously in an event that was correlated within this directive.

This value can also be negated using the symbol [!]. This means that the value of the field has to be different than the value that matched the previous correlation level.



Once the first rule has been configured, the directive will be displayed on screen:



Add a new correlation rule

To add a new correlation rule click on the symbol . The rule will be added to the next level of correlation, just after the level of correlation which contained the symbol that was clicked.

Clone a correlation rule

To clone a correlation rule click on the symbol next to the correlation tule that you wish to clone.

Delete a correlation rule

To delete a correlation rule click on the symbol next to the correlation tule that you want to clone.

Correlation Levels

To change the correlation level of a correlation rule click on the symbols (Move to previous correlation level) and (Move to the next correlation level) next to the rule that you want to move to a different correlation levels.

Rules can also be moved within the same correlation level using the symbols (Move up) and (Move down). Anyway , the position of the rule within the same level of correlation does not imply that the rule has a higher or lower priority.

Modify a Correlation Directive

To modify a correlation directive click on the category containing the directive and then click on the name of the directive.

Clone a correlation directive

To clone a correlation directive click on the category containing the directive and then click on .

Delete a Correlation Directive

To clone a correlation directive click on the category containing the directive and then click on .

Modify the global properties of the Directive

After clicking on the name of the directive and once in edit mode, click on the symbol next to the name of the directive.

Properties

Intelligence -> Correlation Directives -> Properties

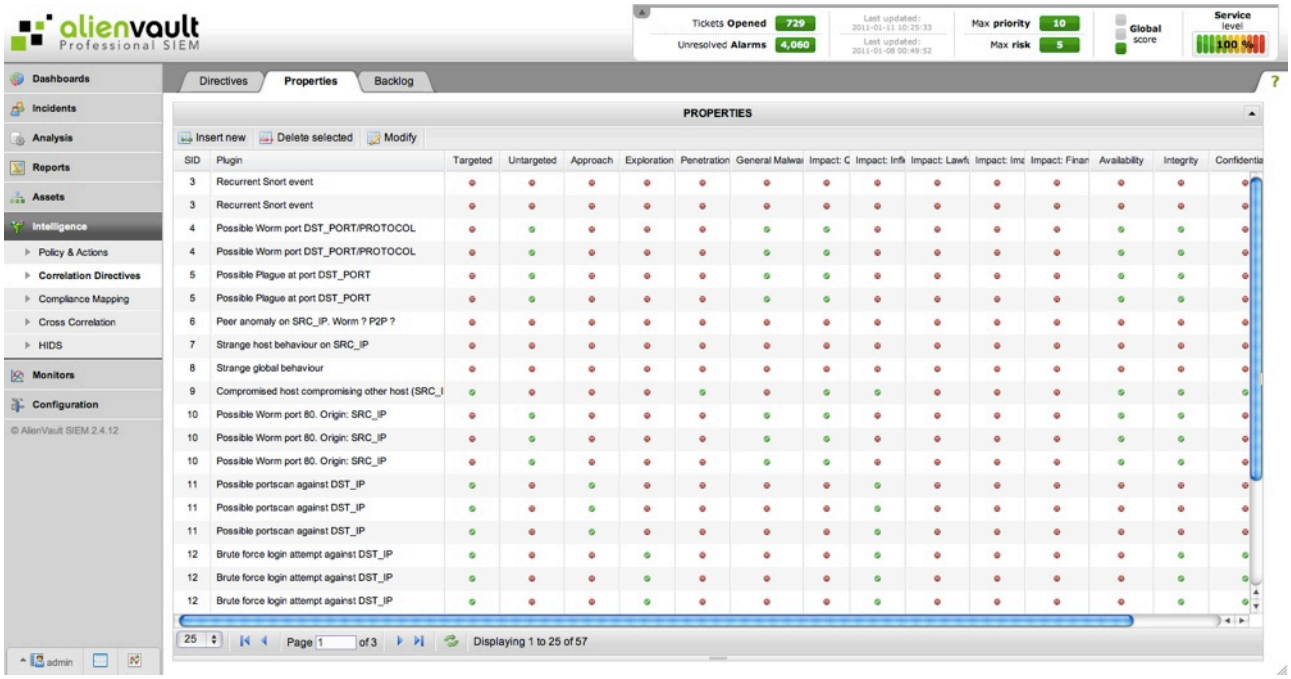
Description

Each correlation rule has properties that are assigned to be used in the reporting system and when displaying statistics.

The properties of the directive describe the consequences that would cause the situation detected by the correlation directive in the corporation that is being monitored.

These are the properties of a correlation directive in AlienVault:

Targeted	Untargeted	Approach	Exploration	Penetration
General Malware	Impact: QOS	Impact: Infleak	Impact: Lawful	Impact: Image
Network Anomaly	Impact: FInancial	Availability	Integrity	Confidentiality



Usage

Insert correlation directive properties

To insert the properties for a new directive click on **Insert New** in the upper left side. A form will be displayed, in this form enter the ID of the directive and then set the properties of the directive, then click on **OK.**

Modify correlation directive properties

To modify the properties of a directive select the directive from the list and then click on **Modify.**

Delete correlation directive properties

To delete the properties of a directive select the directive from the list and then click on **Delete selected.**

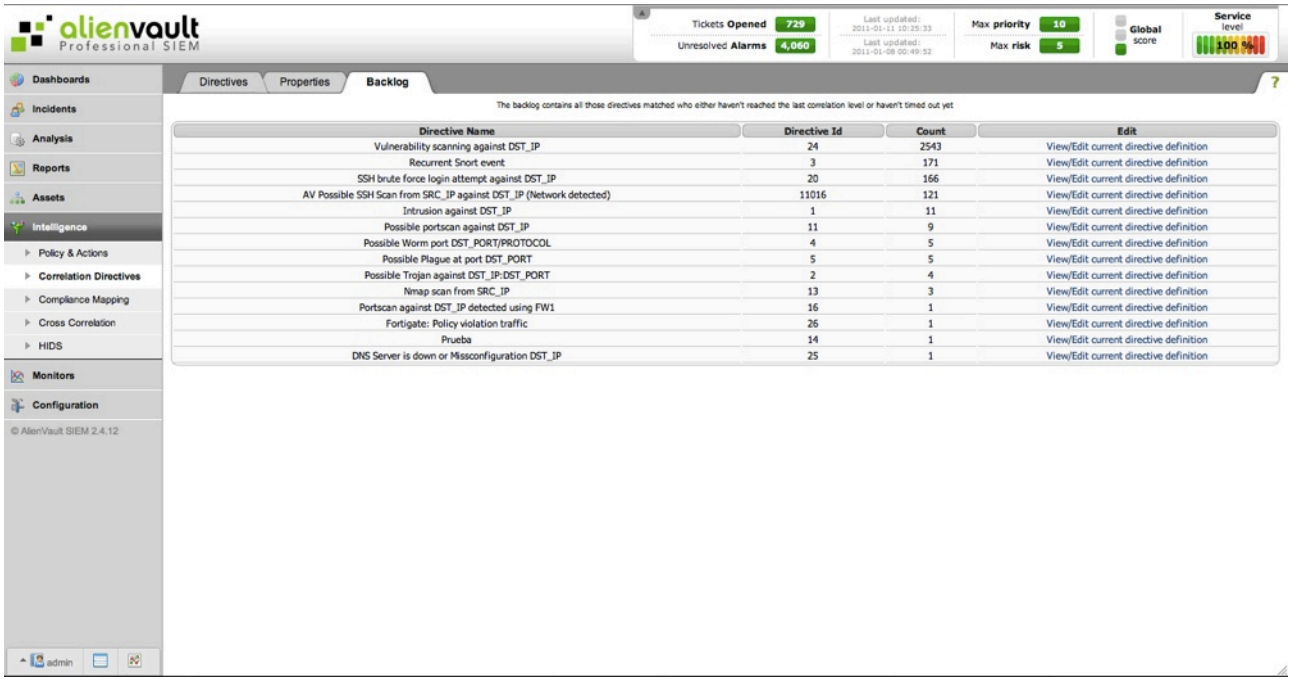
Backlog

Intelligence -> Correlation Directives -> Backlog

Description

The backlog tab displays contains all those directives matched who either haven't reached the last correlation level or haven't timed out yet. The table contains the following fields:

- **Directive Name**: Name of the correlation directive
- **Directive ID**: ID of the correlation directive
- **Count**: Number of events generated during the correlation of this directive.



Usage

To view or edit one of the correlation directives click on **View/Edit current directive definition** within the line displaying the directive that you would like to view or edit.

Compliance Mapping

The Compliance Mapping section is used to define relationships between the compliance control objectives and the AlienVault correlation rules. Most of the compliance control objectives have relationships with correlation directives of the professional feed, so Compliance monitoring with AlienVault makes more sense for those that own the professional feed.

Correlation rules generate new events when the conditions defined in each rule of the directive have occurred. If AlienVault successfully correlates one of the directives, and that means that one of the compliance control objectives is not being met, then that directive should be mapped to that compliance control objective. To do that you should use this section of AlienVault.

After defining all relationships between the correlation directives and the compliance control objectives you will be able to generate a useful Compliance report in the Report section.

ISO 27001

Intelligence -> Compliance Mapping -> ISO 270001

Description

ISO/IEC 27001 is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 27001 specifies a management system that is intended to bring information security under explicit management control.

The control objectives of the standard ISO 27001 are grouped under the following categories:

A.6 Organization of information security
A.7 Asset management
A.8 Human resources security
A.9 Physical and environmental security
A.10 Communications and operations management
A.11 Access control
A.12 Information systems acquisition, development and maintenance
A.13 Information security incident management
A.14 Business continuity management
A.15 Compliance

Usage

In order to have a good compliance report it is important never deleting alarms from the Alarms Panel (***Incidents*** → ***Alarms***). Alarms should be closed once they have been analyzed and confirmed. Delete alarms only in case they are a false positive.

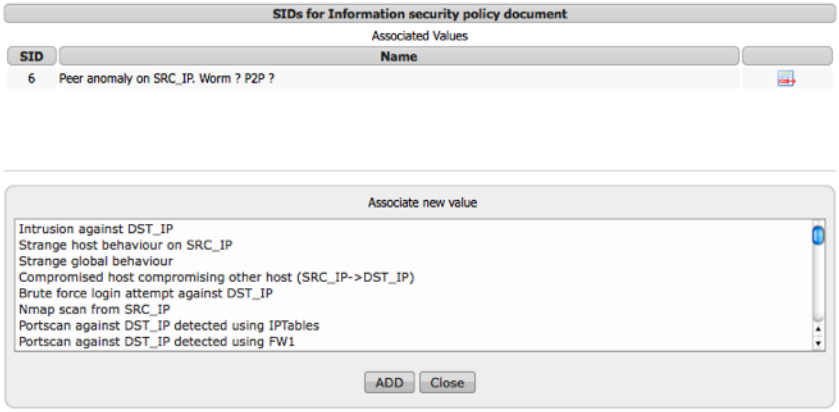
Some compliance control objectives can not be monitored using AlienVault, in that case click on this icon next to the name of the compliance control objective. This way, it will not be included in the Compliance Reports. Disabled compliance control objectives will show this icon in the Operational column, click on it to include it in the report again.

To include a comment regarding one of the control objectives click on in the **Justification** column.

New relationship

In order to define new relationships between compliance control objectives and correlation rules, you just expand one of the listed categories and click on the icon (Plugins column) next to the compliance control objective you want to modify.

In the floating window search and add all the correlation rules that prevent meeting the compliance control objective.



Delete relationship

To delete one of the relationships click on next to the name of the correlation directive. Once you have finished defining the relationships click on **Close**.

PCI DSS

Intelligence -> Compliance Mapping -> PCI DSS

Description

PCI DSS (Payment Card Industry Data Security Standard) was developed by the Payment Card Industry Security Standards Council (Visa, MasterCard…) with the objective of preventing credit card fraud through increased controls around data and its exposure to compromise.

The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

Non-compliant companies, who maintain a relationship with one, or more of the card brands, either directly or through an acquirer risk losing their ability to process credit card payments or being audited and/or fined.

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Usage

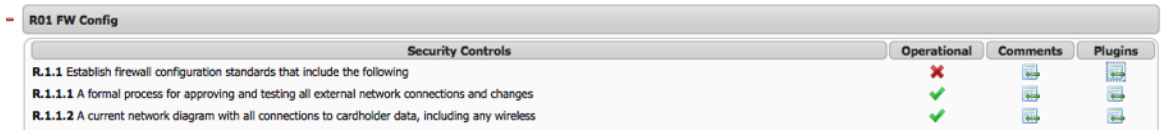
In order to have a good compliance report it is important never deleting alarms from the Alarms Panel (***Incidents*** → ***Alarms***). Alarms should be closed once they have been analyzed and confirmed. Delete alarms only in case they are a false positive.

Some compliance control objectives can not be monitored using AlienVault, in that case click on this icon next to the name of the compliance control objective. This way, it will not be included in the Compliance Reports. Disabled compliance control objectives will show this icon in the Operational column, click on it to include it in the report again.

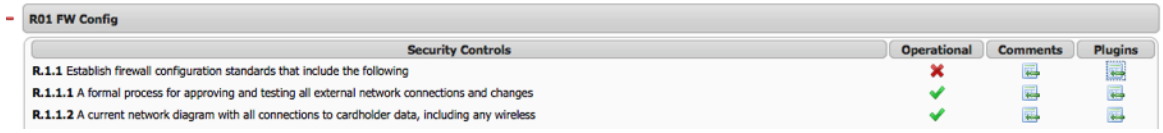
To include a comment regarding one of the control objectives click on in the **Comments** column.

New relationship

In order to define new relationships between compliance control objectives and correlation rules, you just expand one of the listed categories and click on the icon (Plugins column) next to the compliance control objective you want to modify.



In the floating window search and add all the correlation rules that prevent meeting the compliance control objective.



Delete relationship

To delete one of the relationships click on next to the name of the correlation directive. Once you have finished defining the relationships click on **Close**.

Cross Correlation

Cross Correlation

Intelligence -> Cross Correlation -> Cross Correlation

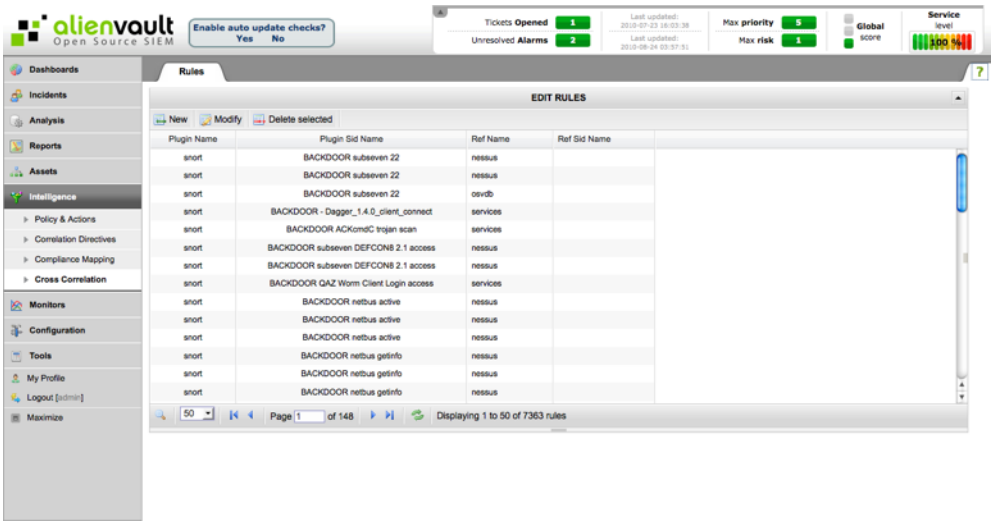
Description

Cross Correlation is AlienVault's ability to correlate across two different plugins. Cross Correlation is used to modify the reliability of an event. Modifying this value will has effect over the Risk, and by extension, the Alarm generation.

Cross correlation is carried out with events that have a defined IP destination address. The reason is that in this kind of correlation, you are going to check if the event destination has some vulnerability defined in the database.

The basic rule for Cross Correlation is: if the IDS (Snort) has discovered an attack to an IP, and you know that the IP has that vulnerability, the reliability will be increased to 10.

Cross-correlation rules included by default basically relate the IDS (Snort) with the Nessus/Openvas events, but any other two events can be correlated using the cross-correlation feature.



Usage

New cross-correlation rule

To insert a new cross-correlation rule, click on **New** in the upper right. A form will be displayed in a floating window. You will have to select the events that will be related using a cross-correlation rule.

On the right side you will have to select the reference event, the one that has to arrive first to the Cross-correlation engine (Usually vulnerability scanner events), on the left side you will have to select the event arriving lately (Usually an IDS event).

Modify a cross-correlation rule

To modify a cross-correlation rule select the rule that has to be modified with a single mouse click, and then click on **Modify**.

Delete a cross-correlation rule

To delete a cross-correlation rule select the rule that has to be deleted with a single mouse click, and then click on **Delete**.

Monitors

Networks

Traffic

Monitors -> Network -> Traffic

Description

To offer the users the ability of monitoring and working with Netflow data, AlienVault has implemented this section based on Nfsen. Apart from including this web interface, AlienVault is also deployed in the default installation Nfdump, which collects netflow data generated by the network devices in your network. In case the network devices in your network do not support netflow, AlienVault is also deployed by default Fprobe, which will generate the necessary Netflow data using after analyzing all incoming traffic (AlienVault Sensor will have to collect all traffic from your network in order to generate Netflow data using Fprobe).

Netflow

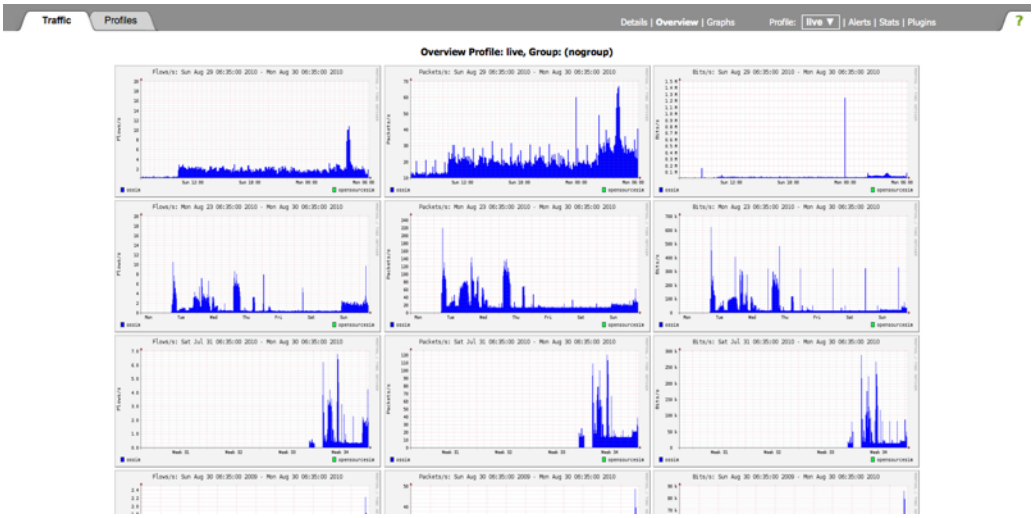
NetFlow is a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting IP traffic information. It is proprietary but supported by platforms other than IOS, such as Juniper routers, Linux or FreeBSD and OpenBSD.

Usage

Tab Navigation

Overview

The default view shows an overview of the currently selected profile. By default, this is the live profile. The three columns show the 'Flows', 'Packets' and 'Bytes' history.



If the currently selected profile is a continuous profile, the page is automatically refreshed every 5 minutes to update the graphs. This allows you to have a browser window on your screen, with always up to date graphs. The Graphs tab adds a sub navigator bar, where you see again the 'Flows', 'Packets' and 'Bytes' graphs but bigger in size. When clicking on one of the graphs in either view, you will be automatically switch to the 'Details' view for further investigation processing.

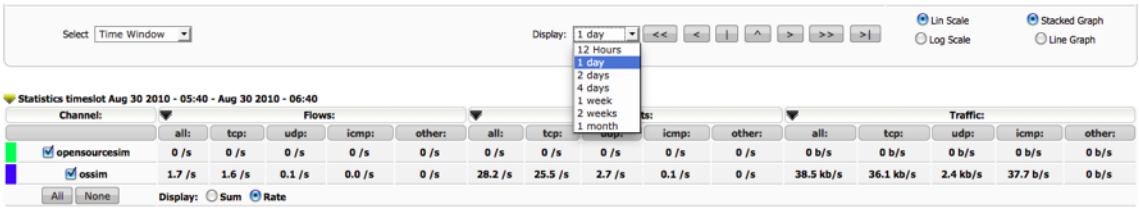
Details

Detailed navigation and investigation of the netflow data is done in the 'Details' view. When entering this view, you will see the navigation display. This will be the default view when entering Monitors → Network → Traffic section.

The page is divided into two parts: The upper part allows you to navigate through the netflow data as well as selecting a single time slot or time window. The lower part contains all the controls to process the netflow data of the selected time slot or time window.

Clicking on any of the small protocol or type graphs will replace the main graphics with the selected graph. You can switch back and forth and select the protocol and/or type for the main graph, which is appropriate for investigating your current situation. The bigger main graph is automatically split into the protocols 'TCP', 'UDP', 'ICMP' and 'other', which is 'not (proto tcp or proto udp or proto icmp)', whenever you switch the type. To 'flows', 'packets' or 'bytes'.

The available time span of the graph can be changed using the pull down menu, just below the main graph:



Selecting a different time slot

A time slot starts at every 5 minutes cycle of the hour (0, 5, 10, 15 etc.) and lasts 5 minutes. On the other side a time window consists of several time slots. When entering the 'Details' view a window scale of one days is selected so you will see the last 24 hours of the profile. The time cursor is placed in the middle of the begin and end of these 24 hours and the time window slot is set to one time slot. You will see the selected time slot or time window always in the title of the browser window, in the title of the main graph as well as above the small type graphs in the upper right section of the main graph. There are several ways to change the current time slot.

The most easiest one is by simply clicking into the graph at the appropriate time slot. This immediately move the cursor to the selected position.

You may also very easily dragging the handle of the cursor to the select time slot within the selected time span.

While moving the handle, the current selected time slot is automatically updated in tstart and tend on the right hand side of the graph. When releasing the handle, the cursor automatically snaps to the nearest time slot and the values in the statistics table are updated accordingly.

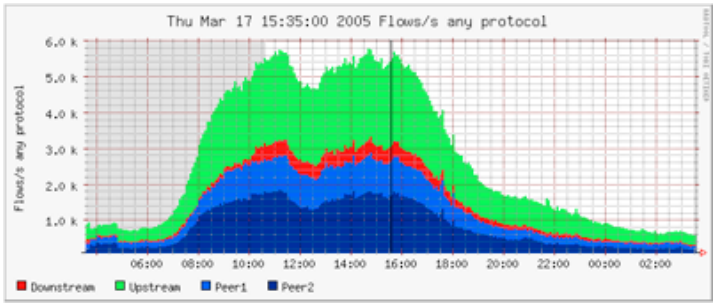
Other ways selecting a different time slot using the control buttons below the main graph:

Using the time cursor controls:

- **>** Next time slot: Advance time by 5 minutes.
- **<** Previous time slot: Go back 5 minutes.
- **»** Advance time slot by a full time span of the graph.
- **«** Go back by a full time span of the graph.
- **>|** Go to the end of the profile. (current time slot)
- **|** Center time cursor in current graph.
- **^** Place cursor at the peak, found within +/- 1 hour time-span of current cursor position.

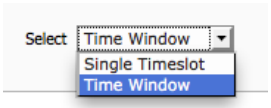
The graphs are immediately updated, when selecting a different time slot. However, there are limits for moving the cursor. The cursor can not be moved outside the visible part of the graph on the left or right hand side. You may also not move the

cursor outside a time slot where data has expired and no data is available for processing. This limit is marked by the dark grey area on the left hand side of the graph.

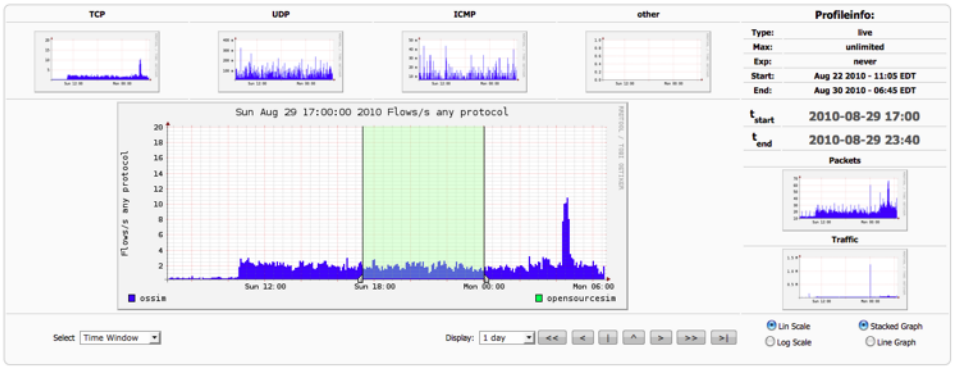


Selecting a time window

Sometimes it is desirable to select and process more than a single 5 min time slot. From the menu below the main graph select 'Time Window'



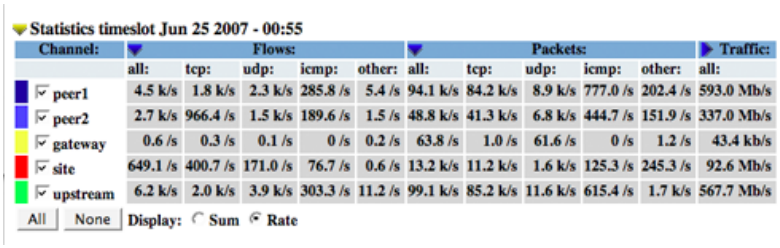
This splits the cursor handle into two halves, which can be dragged individually as needed. Drag the left and/or right border of the selected window as needed.



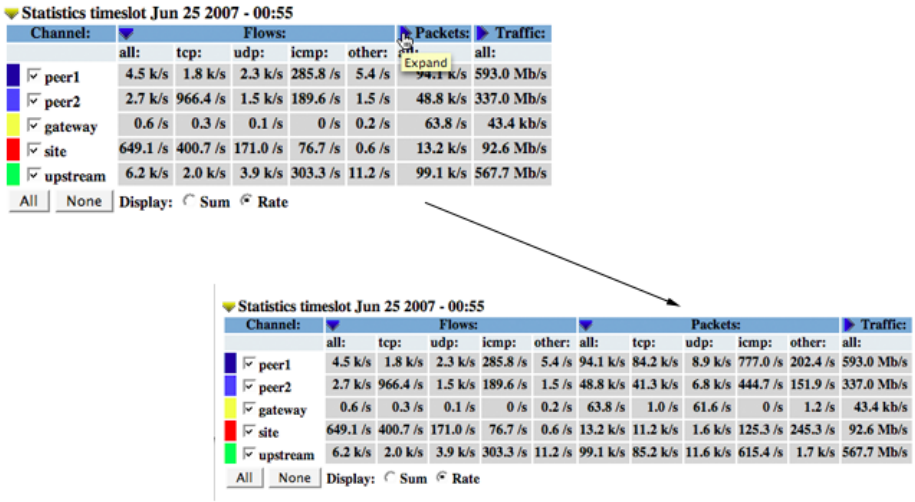
The statistics summary is automatic updated, when releasing either handle, when moving. To switch back to a single time slot, select 'Single Timeslot' from the menu..

Statistic Summary

The statistic summary below the main graph gives you an overview about **flows**, **packets** and **traffic** of the selected time slot or time window. Each line corresponds to one configured netflow source in profile '**live**' or to a configured channel in any other profile. For easy visual matching a small color field with the same color as in the the graph prepends each row. If you are interested in only some of the channels, you may remove the others by clicking the checkboxes. This disables or enables this channel in all graphs and in the statistics respectively. The statistic summary can be switched between the total sum of the selected time window, or the rate values per second. The scaling factors for K, M and G are 1000.



Individual columns can be collapsed or expended as needed, by clicking on the blue triangles. The entire statistics can be shown or hidden by clicking on the yellow triangle. When collapsing a column, a single column remains with the type, which is shown in the main graph.



Enabling or disabling channels re-scales the graphs according the remaining sources, you get a more detailed graph and a different resolution on the y-axis.

Graph Display Options

To view the details your are interested in, a graph may be displayed with different options:

Scale:

- Linear y-axis
- Logarithmic y-axis.

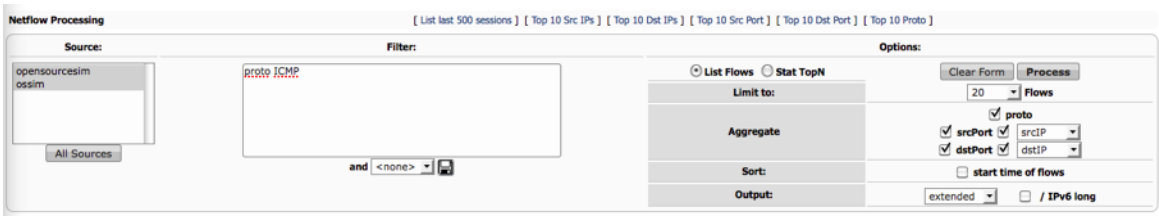
Graph Type:

- Stacked: All sources are drawn on top of each other.
- Line: All sources are drawn independent.

You may switch at any time the display option by clicking on the appropriate radio buttons in the lower right corner of the main graph. You may spot more easily peaks in some of the sources by switching to the line graph display option.

Netflow Processing

Once you have selected the time window of interest, you can process and filter the netflow data according your needs, using the process form in the lower part of the window:



1. Select the netflow sources to process. You may select multiple sources.
2. Enter a netflow filter. The syntax conforms to the nfdump filter syntax.
3. Select any options for the analysis.
4. Click 'process'.

A default filter is supplied when a specific protocol is selected in the main graph. You may add any further filter expressions as needed.

By just clicking **process**, a top 10 statistics of the any IP address ordered by flows is calculated. However, you may change this at any time.

The sources, the filter as well as all options from the processing form are compiled into the appropriate nfdump command. For convenience a short description of the filter syntax and options follows. More details are available in the nfdump(1) man page.

Filter Syntax

The filter syntax is similar to the well known pcap library used by tcpdump. The filter can span several lines. Anything after a '#' is treated as a comment and ignored to the end of the line. There is virtually no limit in length of the filter expression. All keywords are case independent, unless otherwise noted. For a complete filter syntax see the nfdump(1) man page.

Any filter consists of one or more expressions expr. Any number of expr can be linked together:

```
Filter = expr, expr and expr, expr or expr, not expr, ( expr ), not ( expr )

expr can be one of the following filter primitives:
Any
  any Used as dummy filter. Use 'not any' to block all flows.
protocol version
 inet or ipv4 for IPv4 and inet6 or ipv6 for Ipv6
protocol
 proto <protocol> where protocol can be any known protocol  such  as
 TCP, UDP, ICMP, GRE, AH etc. or proto num where num is the protocol number.
IP address
  [SourceDestination] IP <ipaddr> or
  [SourceDestination] HOST <ipaddr> with <ipaddr> as any valid IPv4 or  IPv6  address. Sour-
ceDestination  may  be omitted.
  [SourceDestination] IP IN [<iplist>]
  [SourceDestination] HOST IN [<iplist>]
  iplist space separated list of individual <ipaddr>
[SourceDestination]
 defines the IP address to be selected and can be SRC DST or any combination of SRC and|or
DST.
```

```
 Omitting SourceDestination is equivalent to SRC or DST.
[inout]
 defines the interface to be selected and can be IN or OUT.
network
 [SourceDestination] NET a.b.c.d m.n.r.s for IPv6 network netmask pair
 [SourceDestination] NET net/num with net as a valid IPv4 or IPv6 network and num as mask
bits.
 The  number  of  mask  bits  must match the appropriate address family IPv4 or IPv6. Net-
works
 may be abbreviated such as 172.16/16 if they are unambiguous.
Port
 [SourceDestination]  PORT [comp] num with num as a valid port number.  If comp is omitted,
'=' is assumed.
 [SourceDestination] PORT IN [<portlist>]
 portlist space separated list of individual port numbers
Interface
 [inout]  IF num with num as an interface number.
Flags
 flags tcpflags
 With tcpflags as a combination of:
 A ACK.
 S SYN.
 F FIN.
 R Reset.
 P Push.
 U Urgent.
 X All flags on.
The ordering of the flags is not relevant. Flags not mentioned are treated as don't care. In
order
to get those flows with only the SYN flag set, use the syntax 'flags S and not flags AFRPU'.
TOS
 tos value
 Type of service: Value 0..255.

Packets
 packets [comp] num
 Limit the packet count in the netflow record.

Bytes
 bytes [comp] num
 Limit the byte count in the netflow record.

Packets per second: Calculated value.
 pps [comp] num [scale] to specify the pps of the flow.
Duration: Calculated value
 duration  [comp] num to specify the duration in milliseconds of the flow.
Bits per second: Calculated value.
 bps [comp] num [scale] to specify the bps of the flow.
Bytes per packet: Calculated value.
 bpp [comp] num [scale] to specify the bpp of the flow.
AS
 [SourceDestination] AS num with num as a valid AS number.
[scale] scaling factor. Maybe (Kilo) k, (Mega) m, (giga) g, (Terra) t. Factor is 1024.
          [comp]
The following comparators are supported:
 =, ==, >, <, EQ, LT, GT. If comp is omitted, '=' is assumed.
Examples:
tcp and ( src ip 172.16.17.18 or dst ip 172.16.17.19)
tcp and ( net 172.16/16 and src port > 1024 and dst port 80 ) and bytes > 2048
```

Named Filters

An often used filter can be saved and used at any time later while processing flows. To create such a custom filer, enter the filter in the text box and click on the diskette symbol to save your filter. After successfully saved, the filter is available in the select box. The resulting filter is always the filter in the text box and the named filter, therefore logically linked 'and'.

Options

When processing netflow data, there are two general options. Listing flows and creating a flow statistics. You can switch between the two options by clicking on the appropriate button. Depending on what you have selected, the panel automatically adapts to all available options.

List Flows

List Flows		
Limit to	List only the first N flows of the selected time slot. Equivalent to nfdump option: -c N	
Aggregate	Option to aggregate the flows	By clicking on the checkboxes, you can select how you want to have your flows aggregated. You may also aggregate entire subnets when selecting srcIPv4/<subnet bits>
		By default the flows are not aggregated. Equivalent to nfdump option: -a -A <aggregate options>
Sort	When listing flows from different channels/sources you may sort them according the start time of the flows. Otherwise the flows are listed in sequence of the selected channels. Equivalent to nfdump option: -m	
Output	Select one of the available formats to list the flows. The predefined formats 'line', 'long' and 'extended' are always available and correspond the the output formats of nfdump likewise. However, you may specify any time additional output formats by selecting 'custom …'. Enter your own format now in the text input which appears. The format is equivalent to the format specification described in the nfdump(1) man page.	
	By clicking on the diskette symbol, you save your new format, which appears now in the selection menu, ready to use. For better readability IPv6 addresses are shortened, such as that the middle nibbles are cut and replaced by dots '…' Most often the is good enough to recognize a wanted Ipv6 address your are looking for. If you need the full Ipv6 address, check the option 'IPv6 long'. Equivalent to nfdump option: -o <format>	

Start Top N	
Top	Limit the statistics to the first top N. Equivalent to nfdump option: -n <N>
Stat	Select the statistics you want from the menu and the order option. Equivalent to nfdump option: -s <stat>/<order>
Aggregate	This option is only available for the flow record statistics and is equivalent to the aggregate option in List flows. See the description above. Equivalent to nfdump option: -S
Limit	Limit the output only to those statistic lines whose packets or bytes match the specified limit. Equivalent to nfdump option: -L <limits>
Output	This option is identical to the Output option in 'List flows' . See the description above.

Note: Depending on the size of your network, netflow processing may consume a lot of time and resources, when you select a large time window and multiple resources.

Profiles

A profile is a specific view on the netflow data. A profile is defined by its name, type and one or more profile filters, which are any valid filters accepted by nfdump.

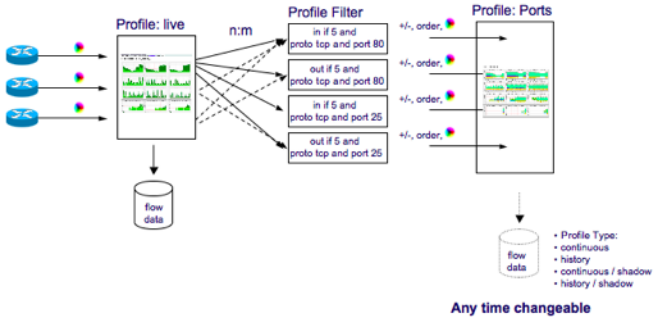
At least the profile 'live' is always available and is used to store your incoming netflow data without filtering. You can switch back and forth to any profile using the pull down menu in the upper right corner of the web page.

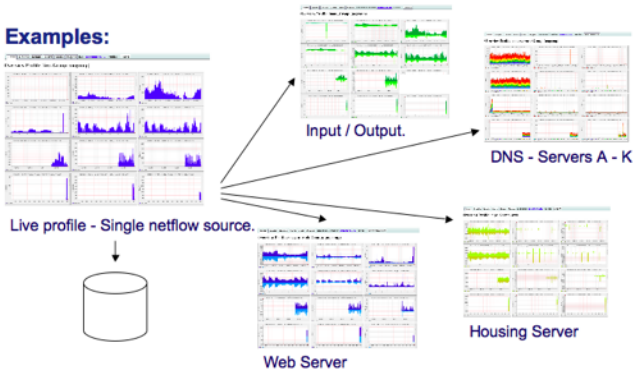
Profile Types

A profile can be either of type **History** or **Continuous**. A history profile starts and ends back in the past and remains static. It neither grows nor expires. A continuous profile may start in the past and is continually updated while new netflow data becomes available. It grows dynamically and may have its own expire values set. Old data expires after a given amount of time or when a certain profile size is reached. Additionally a profile can be created as a Shadow profile, which means no netflow data is collected, and therefore saves disk space. A shadow profile accesses the data of profile 'live' when data processing is done with the proper profile filters applied first.

Profile Channels

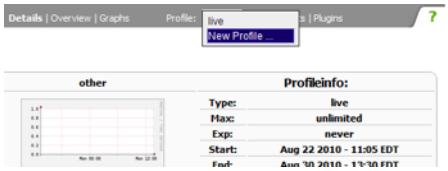
A profile contains one or more profile channels. A profile channel is defined by its channel filter, color, sign and order in which the channel is displayed in the graph. A channel is based on one or more netflow sources from the 'live' profile. The number of channels is independent of the number of netflow sources.





Creating Profiles

Select the “**New profile ...**” entry in the profile pull down menu.



Complete the 'New Profile' form to start building the profile. By moving the mouse over the '?' icon, a help text appears to guide you through the process of creating the profile.

Profiles may be grouped together for easier selection in the profile menu. Select either an existing profile group, or create a new group according to your needs. There is no difference to other profiles other than grouping the profiles in the profile menu.

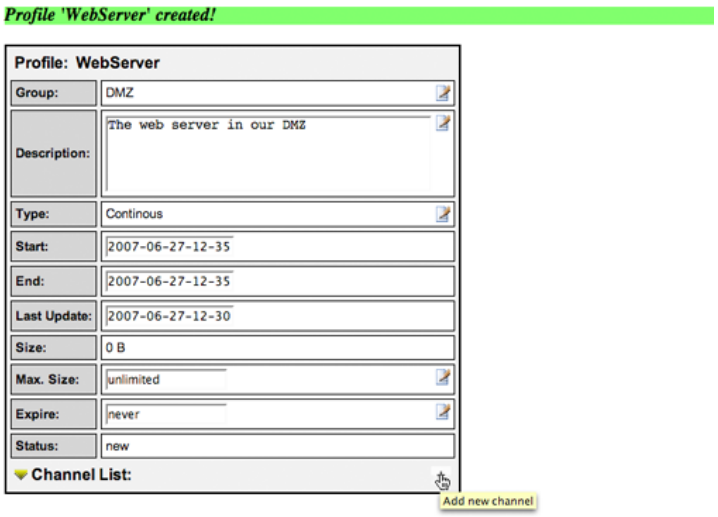
The profile type 'Continuous' or 'History' is automatically detected according the 'Start' and 'End' values you enter. As profiles are created from netflow data from profile 'live', the start and end of the profile must fall in the time range of the profile 'live'.

- If you leave the 'Start' and 'End' inputs empty, a continuous profile is created and starts from the time the profile is created.
- If you enter a 'Start' time but no 'End' time, a continuous profile is created. Data from the past up to to time, the profile is created is profiled and updated immediately when the profile is created.
- If you enter a 'Start' and 'End' time a history profile is automatically created.

Expire / Max Size A continuous profile may expire due to the age of the data or the profile size used on disk. Expiring starts whenever one of the two limits is reached. Expiring ends at the configured value $low_water (in %) in the config file nfsen.conf. By setting any of these values to 0, the limit does not apply.

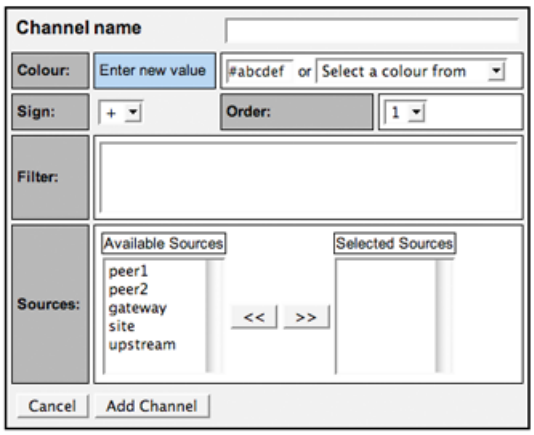
1:1 Profile For compatibility with NfSen version 1.2.x a profile with 1:1 channels may be created, which means, that for every netflow source in the live profile a corresponding channel in the profile will be automatically created. The selected sources and the filter in the profile create dialogue are taken for this 1:1 profile. This is the easiest type of a profile.

Individual Channels For new style profiles select this option. In the 'new profile' dialogue entries for netflow sources as well as for the common filter disappears, as these parameters are now individual for each channel and entered in the channel dialogue.

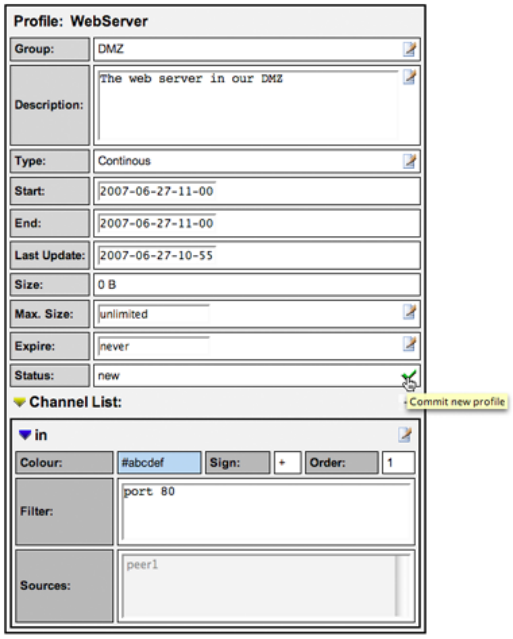


Creating channels

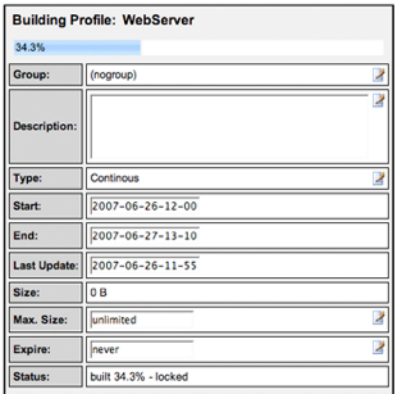
After the profile has been successfully created, one or more channels can be added now by clicking on the '+' icon at the right hand side of the 'Channel List'.



The parameters color, sign and order are used to display the channel correctly in the graph. The filter as well as the netflow sources are needed to correctly profile the channel. The procedure of adding a channel to a new profile can be repeated as often as required to complete the profile. When all channels are added the new profile must be committed to activate the new profile. This is done by clicking on the checkmark on the right hand side of the '**Status**' line.



Once the profile is committed, the build process starts if required. Depending on how long back in the past the profile starts, this can take a considerable amount of time. You can follow the build process by looking at the progress bar, showing you the percentage of completion. This progress bar is updated automatically every 5 seconds. Note: There are no graphs available in the profile as long as the profile is not completely built.



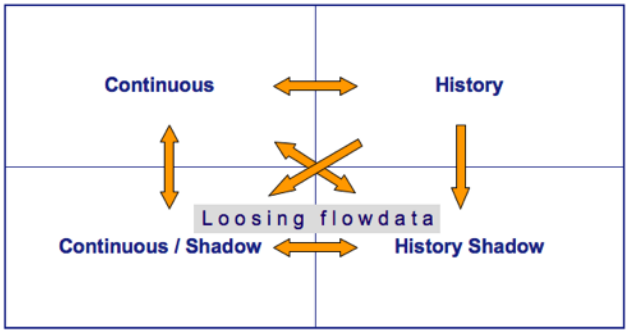
Please note: For the 'live' profile, channels have to be configured in nfsen.conf.

Managing Profiles

Profiles can be modified by selecting the 'Stat' tab of the profile and click on any of the available edit icons of the desired parameter. By clicking on the edit icon of a channel, you may modify the requested channel. All changes will affect the profile immediately. You may also add or delete channels in a continuous profile. However, please note, that adding a new channel to an already existing profile will not rebuild any data for this channel for data in the past. Deleting a channel or the entire profile may be done by clicking on the trash icon.

Converting Profiles

Profile may be converted into another type as desired. However, not all conversions are possible. The figure below shows and explains the possible conversions.



By switching a profile type between continuous and history you may temporary stop collecting data for a profile or continuing to collect data from a stopped profile. Note, that you will loose all netflow data, when a profile is converted to a shadow profile. When switching back, the data recording resumes at the time of switching.

Profiles

Monitors -> Networks -> Profiles

Description

This tab displays the Ntop web administration console. Ntop is installed by default on each of the sensors that make up the deployment of AlienVault. This tab is reliable and useful. It is imperative that the network interface in which Ntop is listening receives all network traffic. This requires using a HUB, a Network tap or configuring a port mirroring or port spanning on the network electronics.

Ntop provides graphs and statistics from the analysis of network traffic being monitored. Ntop also contains a wealth of information about the type of use that is being given to the network, creating a profile that allows you to observe the behavior of each user within the network.

Usage

By default, the system will show the instance of Ntop that is running on the machine that is serving the AlienVault Web interface. To see the Ntop instance running on a different sensor select the sensor in the combo of the upper left. In this combo you can also filter by interface, in case Ntop is listening in more than one interface in the sensor. In case you see your sensor in the combo, or you cannot select your listening interface you should go to **Assets → SIEM Components → Sensors** in order to update the configuration of your sensors or to insert a new AlienVault sensor.

Sessions are viewed through **Monitors -> Traffic**. Sessions are TCP and UDP sessions communications between hosts on a monitored network. They are persistent communications between two hosts (if it is a TCP session). AlienVault monitors session when correlating network data. Ntop collects and presents this session information. There is a Sensor selector and a table listing network sessions in the interface.

The Sensor selector allows the user to choose which sensor session table to view. The selector is the combo-box below the AlienVault menu and above the TCP/UDP Session table. The selector lists sensors and networks. Networks are defined under **Assets -> Networks**.

The Active TCP/UDP Sessions table lists all of the sessions for the selected Sensor. There are ten columns in this table:

- **Client** is the hostname or IP Address of the host talking to a server. A host is any computer, router, printer, or other device attached to a network. There are four fields within this column. The first field is the hostname. Ntop will display a hostname if it can resolve the name via DNS or NetBIOS; else wise it displays an IP Address. The second field is optional and in brackets and tells you how the hostname was resolved. The third field is an optional icon or series icons. Flag icons denote a risk with that particular host, where green is low, yellow is medium, and red is high risk. Finally, the last field is the port number on the host where network traffic is originating. Ntop uses the/etc/services file on the Ntop server to resolve service numbers with service names.
- **Server** is the hostname or IP Address of the host accepting connections from clients. A server typically accepts connections from multiple clients because it offers services to those clients. There are four fields with this column. These fields are the same as the client fields described above (see Client).
- **Data Sent** is the amount of data sent from the client in the current connection. This is given in bytes, Kilobytes (KB), Megabytes (MB), etc.
- **Data Rcvd** (Data Received) is the amount of data received from the server in the current connection. This is given in bytes, Kilobytes (KB), Megabytes (MB), etc.
- **Active Since** is the time and date when this connection started. This time is the time on the Ntop server.
- **Last Seen** is the time the connection was last monitored on the network. This is the time on the Ntop server.
- **Duration** is the time duration of the monitored session. This is in the format hh:mm:ss

- **Latency** is the recorded latency between the client and server.

Global is the global information for the currently selected sensor. This provides an executive overview of Ntop's measurements. This page features a large number of graphs suitable for inclusion in management reports about the current state of the network. Particularly noteworthy, is a link to Historical Data listed under the Traffic Report; here you'll see historical information stored in RRD format.

Protocols lists host traffic categorized by network protocols. The categories include Network and Transport layer protocols from the five-layer TCP/IP model (e.g. ICMP, IGMP, TCP, UDP, etc.). It displays reports the number of bytes sent using each protocol.

Services > By host: Total lists total host traffic categorized by network application. This is a table with a row for each host and data values with the number of bytes sent by each host. The categories are Application layer protocols from the five-layer TCP/IP model (e.g. HTTP, DNS, NETBIOS, etc.). Services > By host: Total is the sum of bytes sent and received by the host. Services > By host: Sent lists the same information, but only sent data. Services > By host: Recv lists the same information, but on received data.

Services > Service statistic displays overview information about protocols and services on the network. This is a combination of tables and charts.

Services > By client-server lists services seen on the network and the hosts using those services. This is a table with rows for each service.

Throughput > By host: Total lists total averages, peaks, and current rates of network traffic. This is a table with rows for each host and data values with the rate for each host in bytes per second (bps). The total is the sum of the bytes sent and received by the host. Throughput > By host: Sent lists the same information, but only sent data. Throughput > By host: Recv lists the same information, but only the received data.

Matrix > Data Matrix is a table listing IP Subnet Traffic.

Matrix > Time Matrix is a table color-coded listing of percentages for traffic of each host on the network by time.

Gateways, VLANS > Gateways lists activity from local subnet routers. It shows the routers that are actively used by any host.

Gateways, VLANs > VLANs lists activity from local Virtual Local Area Networks (VLAN).

OS and Users lists the operating systems and user IDs found on the network. The data inside here hasn't got a direct relation with the Report→Host report information

Domains lists the statistics for all Domains on the network.

Availability

Monitors -> Availability

This tab displays the AlienVault Web administration console. Nagios can be installed in each sensors or a single Nagios can be deployed in the desired sensor. Nagios is an availability monitor that watches hosts and services, alerting users when things go wrong and again when they get better.

When hosts are inserted into the AlienVault inventory, the system can be configured to automatically include the hosts and in Nagios so that the availability of the services running in those hosts can be monitored easily. Note: proceed with caution as it may generate thousands of events and alarms if you are monitoring the entire network and not only the services that should be running all time in your important servers.

If you want hosts to be automatically included in the Nagios configuration make sure you have Nagios enabled in the host configuration in **Assets → Assets→ Hosts**. In this screen you will also be able to select the services that will be monitored by Nagios in each host of your Network.

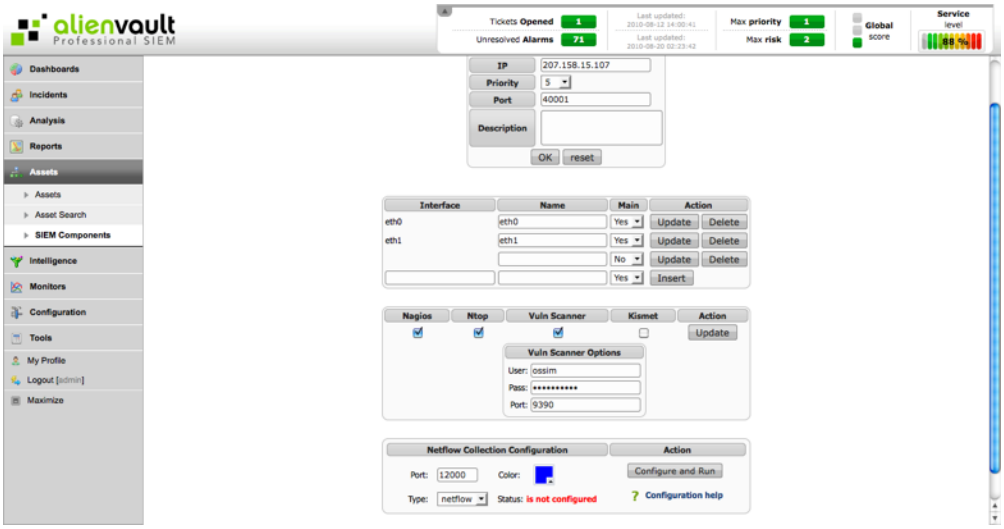
Nagios can also work as a detector plugin in AlienVault, this means that the events generated by Nagios can also be stored in the Forensic database and that directives can be defined using the events that are being generated by Nagios and collected by the AlienVault Agent (AlienVault Collector).

Usage

There is a Top menu that has a number of options to view data. These options are accessible for all Sensors. The details are divided between Monitoring and Reporting.

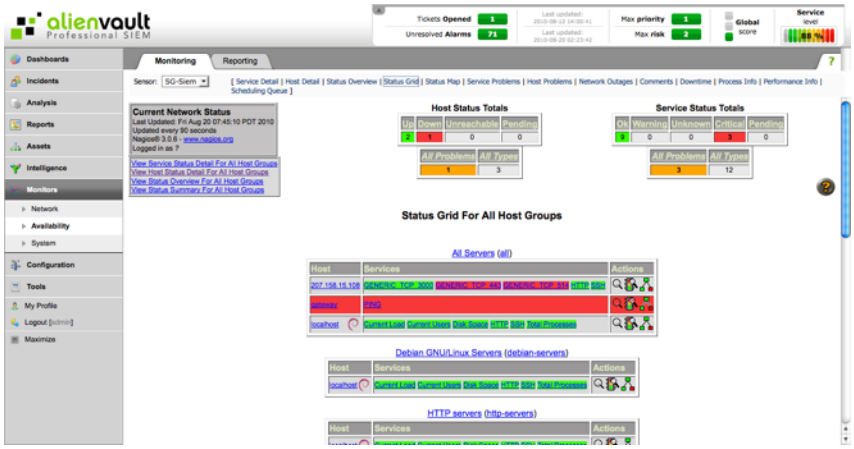
The Sensor selector allows the user to choose which sensor to view data. The selector is the combo-box at the top of the left sidebar. The selector lists hosts where the AlienVault Sensor is installed.

If you don't find a sensor in this combo-box, make sure Nagios is enabled for this sensor going to **Assets → SIEM Components → Sensors**



Monitoring

- **Service Detail** lists the details of monitored network services. This includes services like http and ftp.
- **Host Detail** lists the details of monitored hosts. This provides details of various statistics collected by the Nagios agents.
- **Status Overview**, **Status Grid**, **Status Map**, **Service Problems**, **Service Problems**, **Host Problems**, **Process Info**, and **Performance Info** all provide different views into comprehensive information for the sensor. These features allow users to see problems with their network assets in one place.
- **Comments** allows administrators to share information about various assets.
- **Scheduling Queue** is where various nagios jobs are scheduled. Nagios runs processes at various times and this is where that is configured. This includes when services are checked among other things.



Reporting

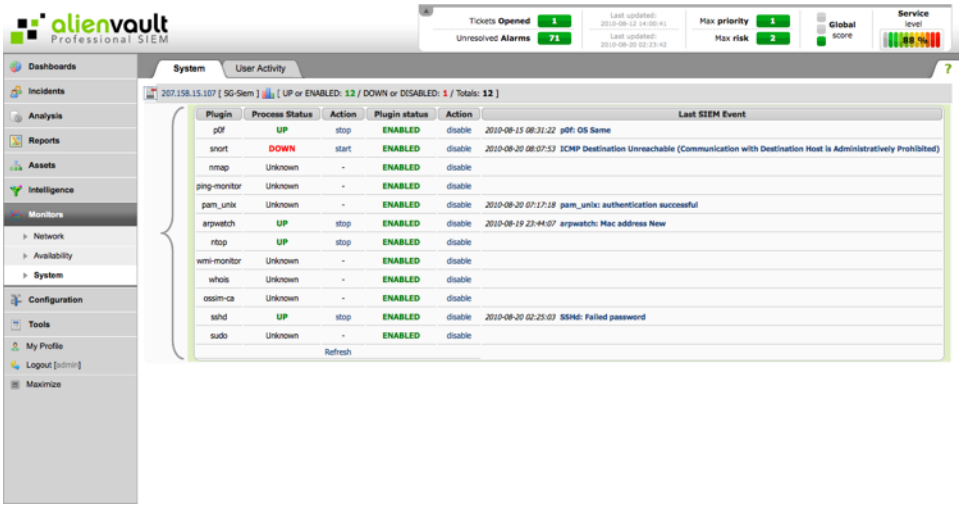
- **Trends** reports with graphs the various state of assets over a period of time.
- **Availability** reports on the readiness of assets over a period of time.
- **Event Histogram** reports with a graph the availability of an asset over time.
- **Event Summary** has generic reports about host and service alert data. This includes alert totals, top alert producers, and a number of other metrics.
- **Notifications** displays messages that have been sent to various contacts in nagios database. These messages are used to forward information about a specific asset to specific persons.
- **Performance Info** is a collection of MRTG graphs illustrating various statistical data for monitored assets.

System

System

Monitors -> System -> System

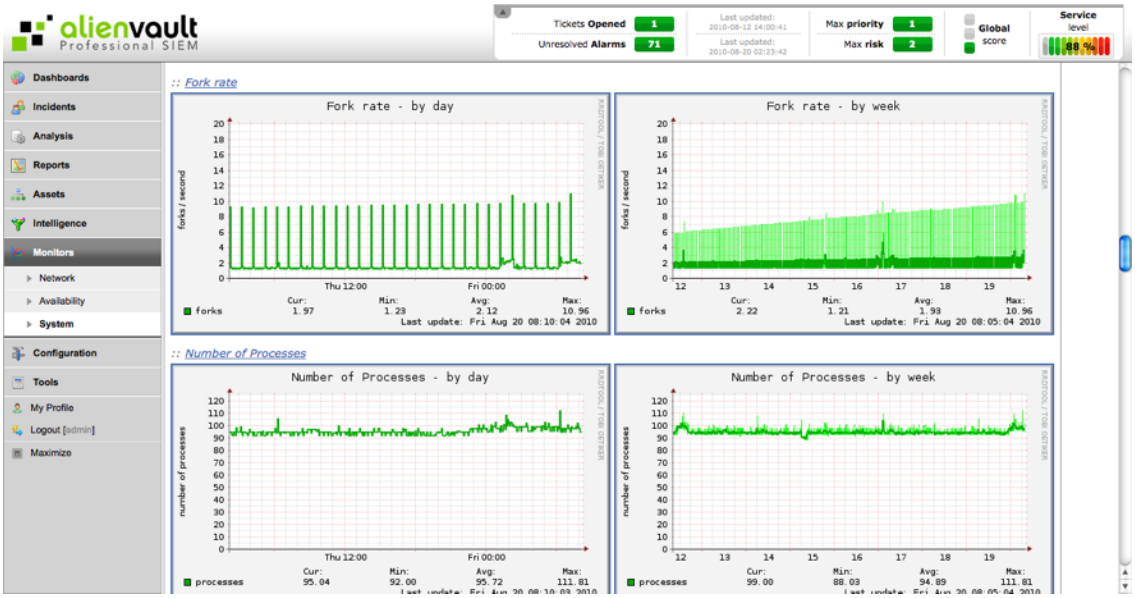
This tab shows all the Sensors connected to the AlienVault Server. In case not all your Sensors are displayed, go to **Assets→ SIEM Components → Sensors** and insert the information of the missed Sensor. Sensors are used to collect information from the different applications and devices in the network. In some cases the applications will be running in the same box that the AlienVault Sensor resides, and in some other cases, the sensors will collect information from the devices using SNMP, Syslog, FTP, Samba or any other collecting method.



There are five columns to the sensor status table.

- **Plugin** is the name of the plugin installed and configured on the sensor. A plugin is the mechanism through which AlienVault receives data. The plugin is responsible for parsing incoming data on the sensor and normalizing it into a format that AlienVault understands.
- **Process Status** indicates whether or not the plugin is operational. A green **UP** indicates that the plugin is running and sending information to AlienVault. A red **DOWN** indicates that the plugin is not running. A black Unknown indicates that the sensor cannot determine the status (this is not necessary a bad thing as the application may not be running in the same box that the Sensor is doing)
- **Action** (at the right of 'Status') is a hyperlink that may be used to change the state of the plugin. Start hyperlinks attempt to start the corresponding plugin. Stop hyperlinks attempt to stop the corresponding plugin. These commands are executed only on the corresponding sensor.
- **Enabled** indicates whether or not the plugin is active and reporting. The plugin may be disabled in the agent configuration file. The sensor's built-in watchdog does not monitor disabled plugins. Furthermore, it may be disabled in from the following action column.
- **Action** (at the right of 'Enabled') is a hyperlink that may be used to change the status of the plugin. Disable turns off a plugin and stops it from auto starting when the sensor reboots. Enable turns on a plugin and starts it when a Sensor reboots.

When clicking on this icon  shown in each line (One line per Sensor) you can access Munim. Munim is a tool that helps analyzing resource trends and monitor performance providing a lot of graphs to monitor the system performance. Munim is installed by default in each Sensor of the AlienVault deployment.

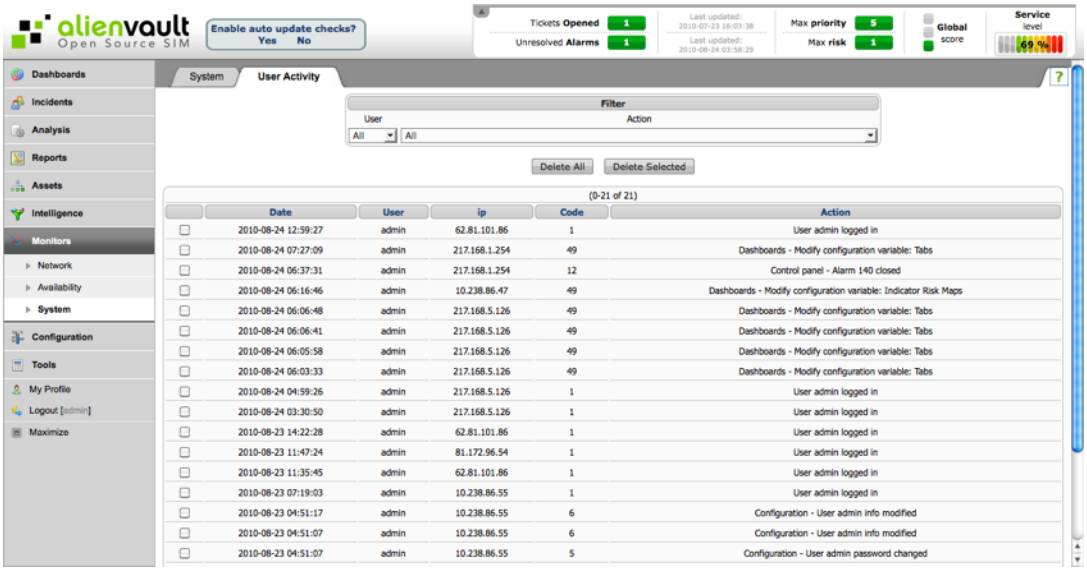


User Activity

Monitors -> System -> User Activity

Description

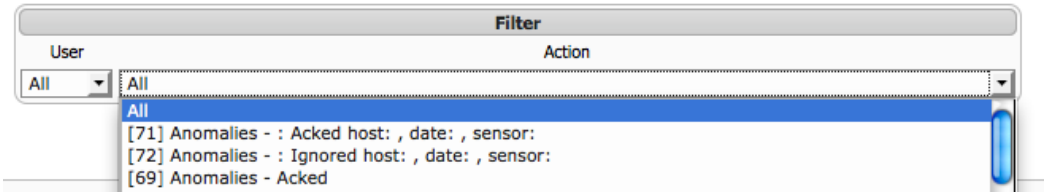
The User Activity section displays a record of user activity within AlienVault console. This allows for keeping track of user accesses to the AlienVault Web interface, as well as configuration changes. The admin user will have permissions to delete records on this screen, so be sure to only have one admin user in your corporation to avoid continuity problems.



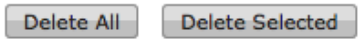
It is possible to configure what actions have to be logged in this section in **Configuration → Users → User Activity**.

Usage

The upper form can be used to filter by user or by action.



The admin user will also have permission to delete certain records or all records shown on this screen.



Configuration

Main

Configuration -> Main

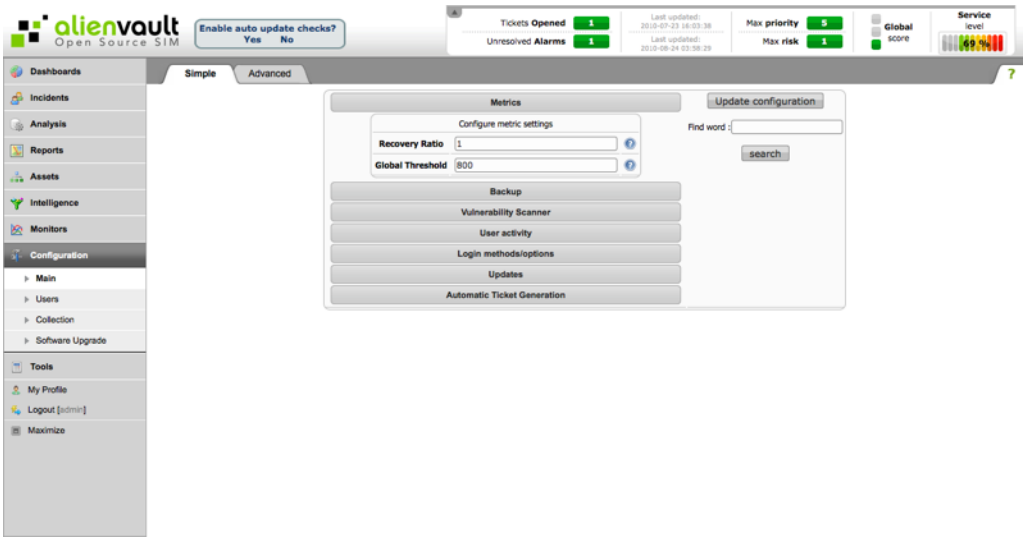
Description

The Configuration section allows you to set appearance and general system settings. Notice that many of the settings are also modified by **AlienVault-reconfig** script and should not be modified unless you know what you are doing. If you are facing any problem using AlienVault please refer to the professional support or ask for help in the forums before modifying advanced configuration parameters. As AlienVault integrates many software packages a single change in configuration could affect many AlienVault components

Configuration options have been categorized into in Simple and Advanced Configuration.

Usage

To change the value of one of the configuration parameters, click on the category, insert the new configuration value and click on **Update configuration**.



Simple Configuration

Language	
Language	Web interface default Language
Metrics	
Recovery Ratio	Recovery value for Compromise and Attack (subtracted every 15 seconds)
Global Threshold	Global Threshold Value (Compromise and Attack)
Backup	
Forensics Active Event Window	Number of days stored in the SIEM database
Vulnerability Scanner	
Vulnerability Ticket Threshold	Minimum risk that a vulnerability has must have to automatically open a ticket in the system
User Activity	
Enable User Log	Log user actions within the AlienVault Web interface
Log to Syslog	Log user actions to Syslog
Login Methods / Options	
Show welcome message at next login	Show welcome message
Require a valid AlienVault user for login	Allow login for not defined users (When using LDAP)
Enable LDAP for login	Enable LDAP authentication
Ldap server address	IP address of the LDAP server
LDAP CN /LDAP O/LDAP OU	LDAP configuration parameters
Password Expire	Require a password change after N days
Updates	
Enable auto update-checking	Check for updates automatically (Requires internet connection)
Tickets	
Open Tickets for new alarms automatically?	Open tickets automatically whenever an alarm happens

Advanced Configuration

Language	
Language	Web interface default Language
Locale file directory	Directory containing localization files
AlienVault Server	
Server Address	AlienVault Server listening address
Server Port	AlienVault Server listening port
SIEM	Enable/Disable SIEM functionality
Qualification	Enable/Disable Risk assessment features
Correlation	Enable/Disable correlation
Cross-correlation	Enable/Disable Cross correlation
SQL Storage	Enable/Disable SQL Storage
Logger	Enable/Disable Logger functionality (Available in Professional SIEM)
Sign	AlienVault Server event signing mode (Available in Professional SIEM)
Forward Alarms	Enable/Disable Alarm forwarding functionality (Available inProfessional SIEM)
Forward Events	Enable/Disable Event forwarding functionality (Available inProfessional SIEM)
Alarms to Syslog	Log Alarms using Syslog (Available in Professional SIEM)
Remote Logger	Enable remote Logger console
Remote Logger user	Remote Logger username (AlienVault Web interface)
Remote Logger password	Remote Logger password (AlienVault Web interface)
Remote Logger AlienVault url	Remote Logger URL
Metrics	
Recovery Ratio	Recovery value for Compromise and Attack (subtracted every 15 seconds)
Global Threshold	Global Threshold Value (Compromise and Attack)
Backup	
Forensics Active Event Window	Number of days stored in the SIEM database
Vulnerability Scanner	
Vulnerability Ticket Threshold	Minimum risk that a vulnerability has must have to automatically open a ticket in the system
User Activity	
Enable User Log	Log user actions within the AlienVault Web interface
Log to Syslog	Log user actions to Syslog
Login Methods / Options	
Show welcome message at next login	Show welcome message
Require a valid AlienVault user for login	Allow login for not defined users (When using LDAP)
Enable LDAP for login	Enable LDAP authentication
Ldap server address	IP address of the LDAP server
LDAP CN /LDAP O/LDAP OU	LDAP configuration parameters
Password Expire	Require a password change after N days
Updates	
Enable auto update-checking	Check for updates automatically (Requires internet connection)

Tickets	
Open Tickets for new alarms automatically?	Open tickets automatically whenever an alarm happens

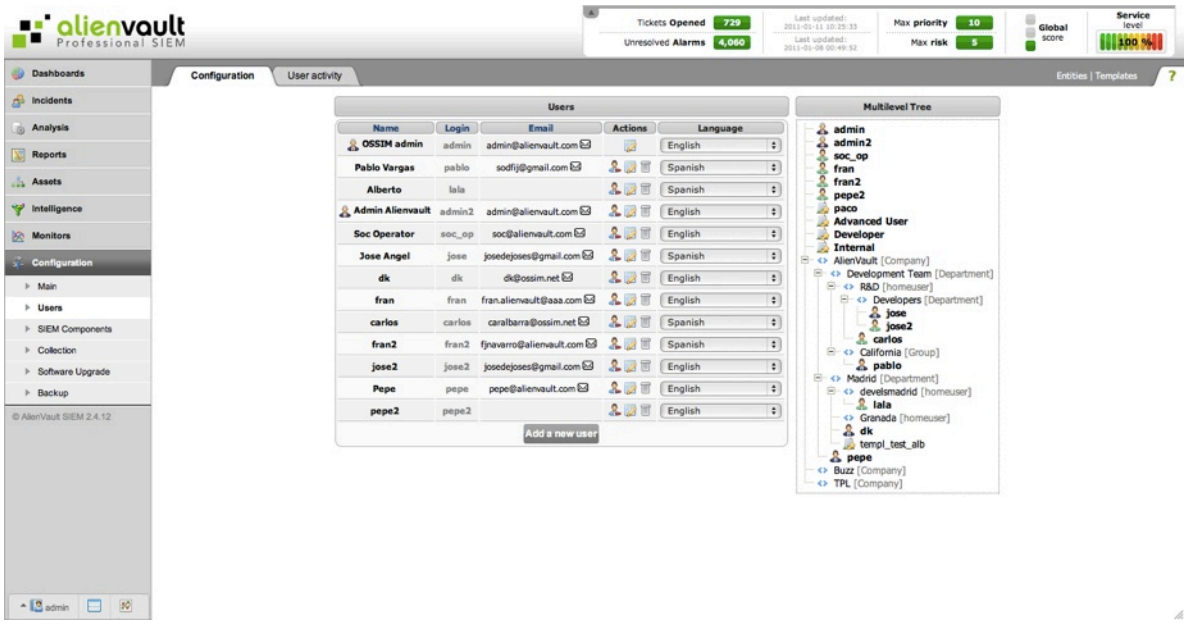
Users

Configuration

Configuration -> Users -> Configuration

Description

To access the information collected and generated by AlienVault, you must have a user in the AlienVault Web Interface. The installation creates a default user that allows for access to the Web interface for the first time to create and set permissions for other users.



The default username is **admin**, with **admin** as password. After the first successful login with the admin user, you will be prompted to change the password for this user.

This user will always keep that special permissions, for this reason it should not be shared and should always be used the admin user or the person in charge of maintenance and management of the AlienVault deployment.

Setting user permissions allows you to limit the information that will be displayed for that user (Assets that the user can monitor) as well as disable or disable certain characteristics of the AlienVault Web interface.

The main difference when managing users between the AlienVault Open Source version and the AlienVault professional version is that in the Open Source version permissions are assigned directly to users while Professional version permits assigning to templates that can be reused for more than one user.

The AlienVault Professional version also allows the creating of entities to create a new virtual layer that groups assets (Networks, Sensors, Network Groups, Hosts, Host Groups ...)

Users

To successfully configure the users within the AlienVault web interface it is important to have a good inventory of the networks that are being monitored.

The assignment of permissions for a user is performed based on the networks that the user can monitor. It is also possible to assign permissions based on the sensors, so that a user has access to all information that has been collected by individual AlienVault Sensors.

For this reason it is important to relate every asset in the inventory (Hosts, Host Groups, Networks and Network Groups) with the sensor or sensors that can collect events generated or in which this asset is involved.

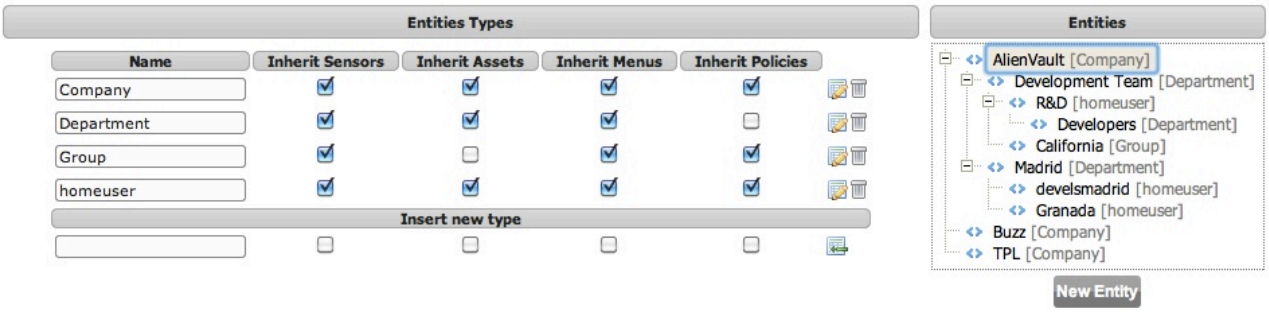
Entities

PRO ONLY

In order to simplify the management of complex AlienVault deployments, AlienVault (SOC, MSSP, Big corporations...) with multiple organizations, departments being monitored where there are multiple users, the professional version allows the creation of entities that greatly simplify the management of user permissions in these complex environments.

An entity is a virtual grouping of objects within the AlienVault inventory (Hosts, Host Groups, Networks and Network Groups...).

Entities can be used to create departments, organizations, companies, or whatever kind of group is needed to simplify the asset management.



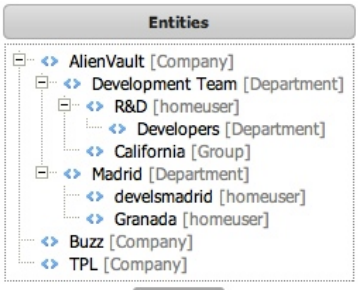
AlienVault stores all the entities using a tree, with all entities that can be monitored using the AlienVault deployment. This way the Entities can be configured to inherit permissions or assets from bigger entities.

Usage

Entities

To create or modify entities click on **Entities** in the upper right. This will display a screen with two tables. The table on the left shows the entities types that have already been created within this AlienVault deployment, and the left side shows a tree with all entities that have been configured in AlienVault.

Entities are shown using a tree with branches. This allows to easy viewing of dependencies between all entities.



New entity type

To insert a new type of entity use the form at the bottom left. You will have to select wether you want the entity type to inherit permissions from an upper entity in case this entity is below another entity.

Click on  to insert the new entity type.

Modify entity type

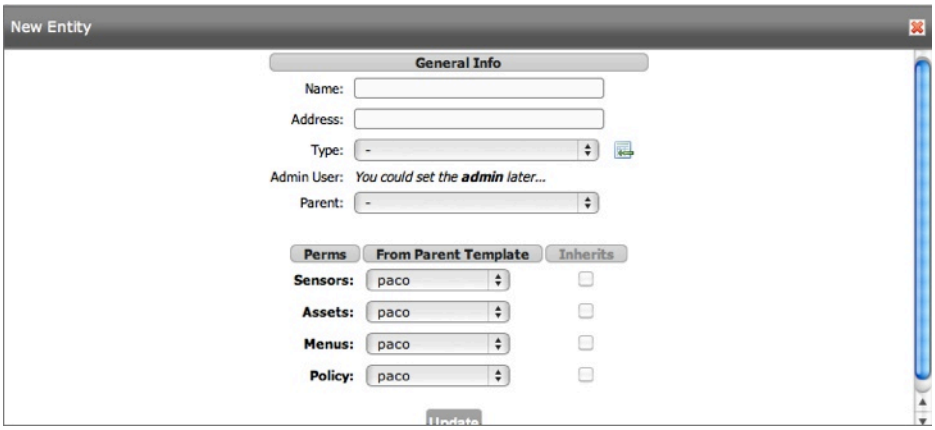
To modify an entity type click on  next to the entity that you wish to modify.

Delete entity type

To delete an entity type click on  next to the entity that you wish to delete.

New entity

To insert a new entity click on the button **New Entity** below the tree.



You will have to enter the following properties for the new entity:

- **Name**: Name of the entity
- **Address**: Physical address in which the assets belonging to this entity can be found
- **Type**: Type of entity
- **Admin User**: User administrator of this entity.
- **Parent**: Parent entity in case this entity belongs to a bigger entity Eg: A department within a company.

The permissions for this entity have to be assigned using from one of the user templates:

- **Sensors**: Sensors that users within this entity can monitor
- **Assets**: Assets that users within this entity can monitor
- **Menu**: Menu options within the AlienVault Web Interface that users within this entity have access to

Modify entity

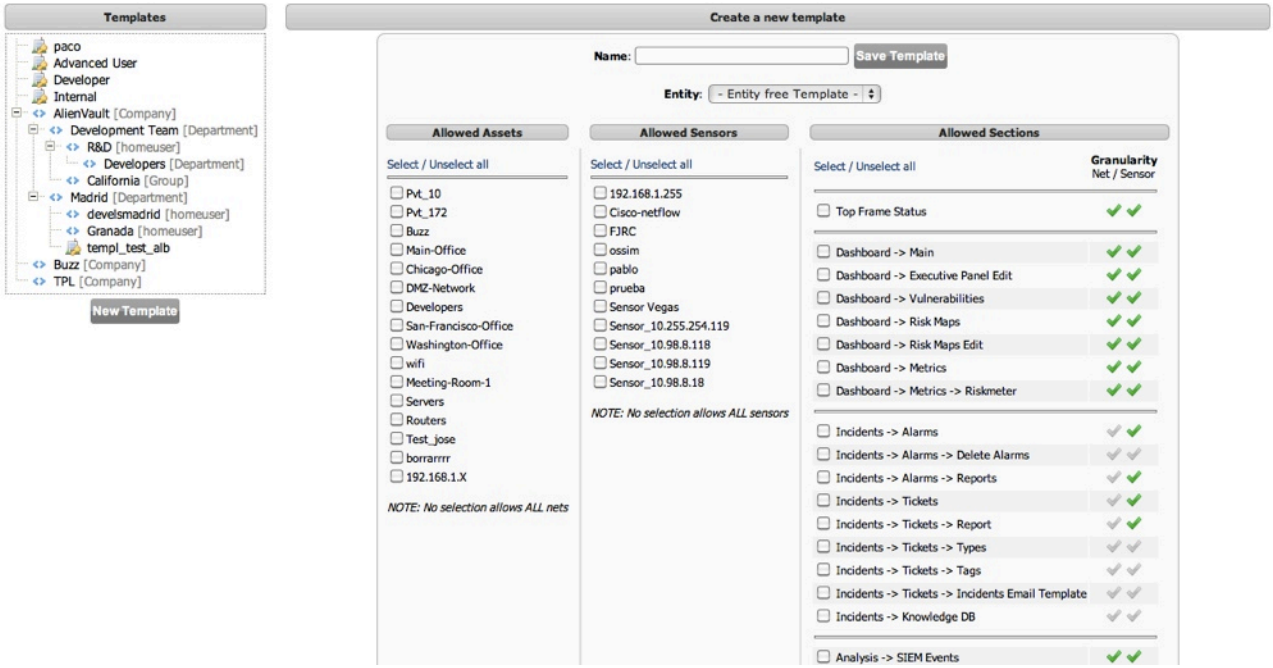
To modify an entity click on the name of the entity displayed in the tree.

Delete entity

To delete an entity click on the name of the entity displayed in the tree, then click on the button **Delete** below the form.

Templates

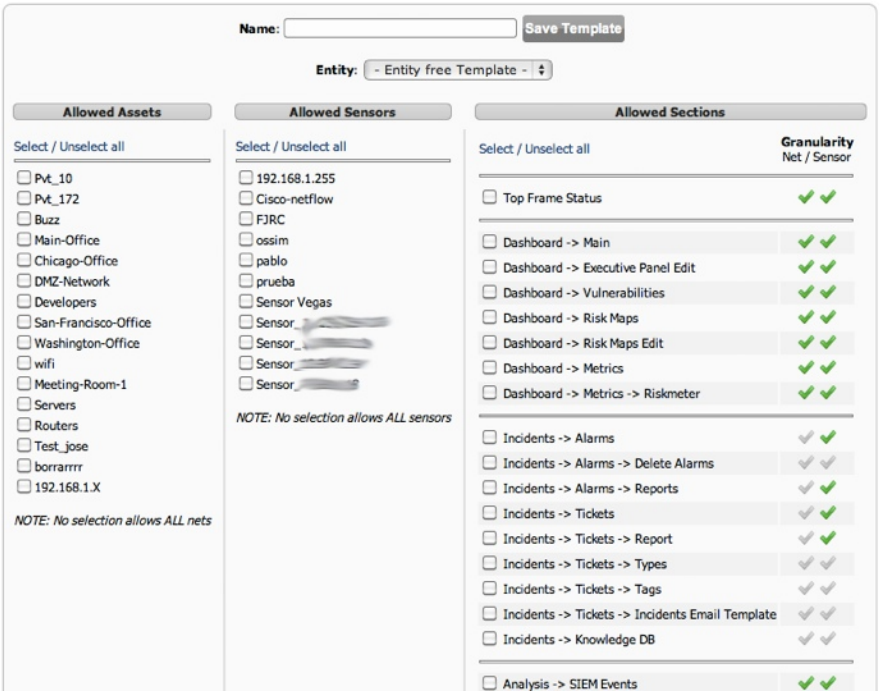
To create or modify user templates click on **Templates** in the upper right.



New template

To create a new template click on the button **New Template** in the bottom left.

Enter the name of the template and select the entity in which you would like to include this template, or select **Entity free template** from the drop-down menu to assign this template to an entity later.



Then select the Networks that the users using this template will be able to monitor, as well as which sensors will collect events that users will see in the AlienVault Web interface.

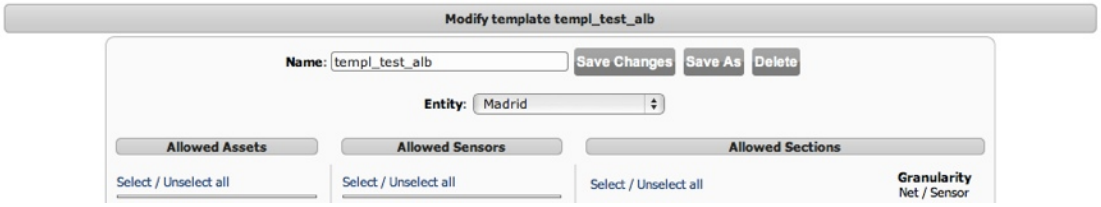
The menu options shown in the AlienVault Web Interface can be limited in each user template. Mark the checkboxes corresponding to the sections you want to give access to the users taking their permissions from this user template.

Modify template

To modify a template select the template from the tree on the left side by clicking on the name of the template.

Delete template

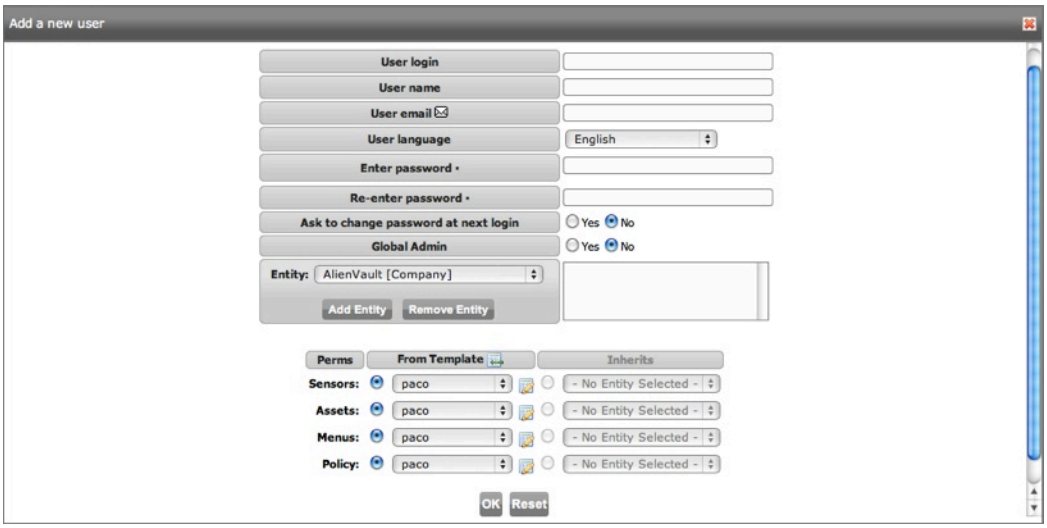
To delete a template select the template from the tree on the left side by clicking on the name of the template. Then click on the **Delete** button.



Users

New user

To add a new user click on **Add New User** below the list of users.



Fill in the values for the following properties

- **User login**: Nickname that the user will use to login
- **User name**: Real user name Eg: Peter Collins
- **User email**: E-mail address of the username that will be used to send notifications, reports... to the user
- **User language**: Language of the AlienVault Web Interface (English, Spanish, French, German, Japanese, Russian, Brazilian Portuguese, Simplified Chinese or Traditional Chinese)
- Ask to change password at next login: Force a password change after the next successful login of the user
- **Global admin**: Whether the user is a superuser within the AlienVault Web interface or not. (Permissions to see all assets and all menu options). Admin users will be represented with this icon whenever the list of users is displayed.
- **Entity**: Choose the entity or entities this user belongs to. Select the entity from the drop down menu and click on **Add Entity.** Select the entity from the right side and then click on **Remove Entity** to remove the user from that entity.

Then assign the permissions for the new users using the user templates created previously

Modify user

To modify a user click on next to the user that you want to modify.

Delete user

To delete a user click on next to the user that you want to delete.

Enable / Disable users

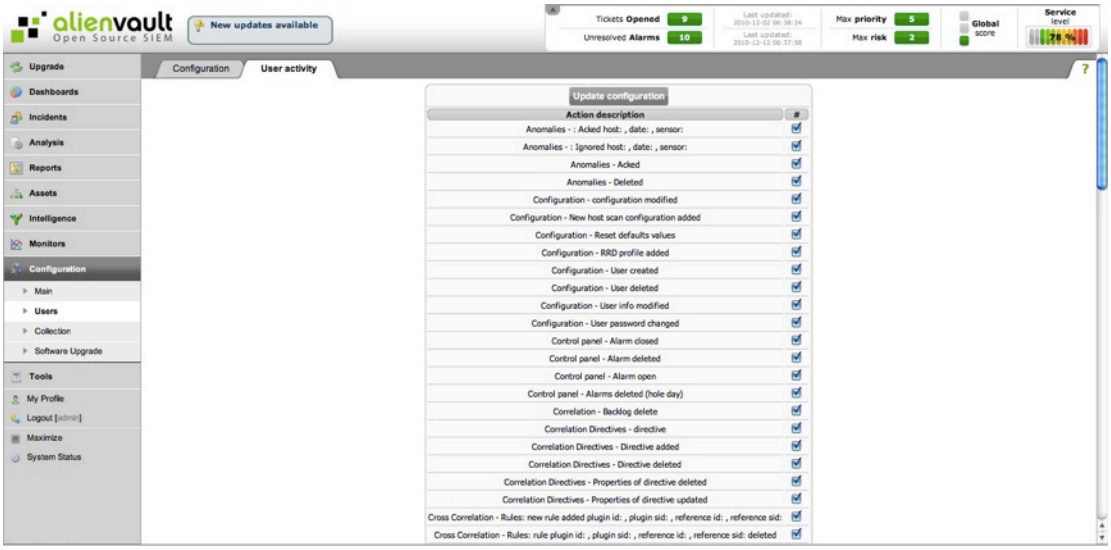
To enable a disabled user on the icon in the user list. Click on to disable a user.

User Activity

Configuration -> Users -> User Activity

Description

This tab lets you configure the user activities within the AlienVault Web interface to be logged. This log can be viewed on the tab User Activity (Monitor -> System -> User Activity)



Usage

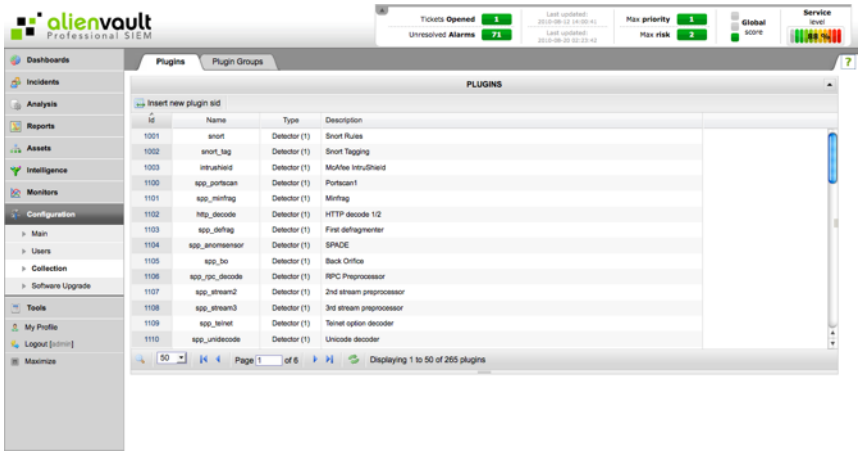
Mark the checkboxes next to the activities that you wish to log and click on **Update Configuration.**

Collection

Plugins

Configuration -> Collection -> Plugins

Plugins are used by AlienVault to improve the collection capabilities of the AlienVault Sensors, telling the system how to understand, and to collect events generated by each application and device. Plugins help with collecting and normalizing events. In order to calculate a risk for every event arriving to the AlienVault Server, the system needs to know every possible type of event that can be collected by the system. This screen shows all the events that the AlienVault server is ready to process. The AlienVault Server retrieves the list of events that may arrive to the AlienVault Server from the AlienVault database.

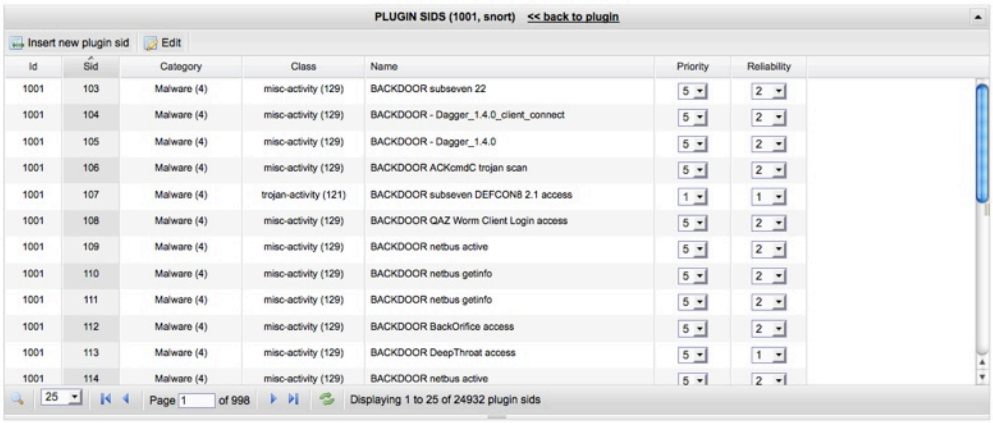


Usage

The **Id** (Plugin ID), is the internal number AlienVault uses to identify the type of device or application that generated the events. The Plugin ID is a unique number that is also used when creating correlation directives or when defining policies to filter certain events. Each type of event is always identified using the Plugin ID (Identifies the tool that generates the event) and the Plugin SID (Identifies the type of event within the tool described by the Plugin ID). The same Plugin SID can be used in different Plugin ID's.

All the events that can be collected for each plugin can be seen by clicking on the ID column.

- The **Name** is the name of the plugin assigned to the plugin ID. This may be any string, but should be descriptive.
- The **Type** is the type of plugin. There are two possible values. Detector is a plugin type that AlienVault uses to send data to the server.. Monitor is a plugin type that AlienVault queries for information.
- The **Description** is additional information used to clarify a plugin's purpose. This is very helpful when a plugin has a particularly obscure name.



Plugin SID is the internal number AlienVault uses to track various messages from sensors. For example, there is a unique Plugin SID for each alert that snort generates . Some parameters for SIDs may be edited here:

- The **Plugin** is the internal number AlienVault uses to track various plugins. Each plugin has a unique plugin ID. Each plugin uses this number and its sub-ID.
- The **Sid** number is used by AlienVault to discriminate individual plugin messages.
- The **Name** is a string assigned to the SID. This may be any string, but should be the close to the message generated by the sensor.
- The **Priority** is a number used to qualify AlienVault alerts with varying levels. It is a numeric value ranging from 0 to 5. 0 is the lowest priority and indicates that AlienVault should ignore that SID. 1 is the the lowest priority while 5 is the highest.
- The **Reliability** is a measure of rule dependability. It is a value from 0 to 10 where 10 is the most dependable and 0 is the least. Reliability is read as a tenth of a percentage. i.e. 4 means there is a 40% chance that this rule is accurate at this stage of the directive.
- The **Action** column contains a Modify button. Clicking the button saves changes to the Priority and Reliability column in the AlienVault database. At this time is necessary to change plugin SID by plugin SID, this means that you can change the Priority or Reliability value just for one plugin SID each time.

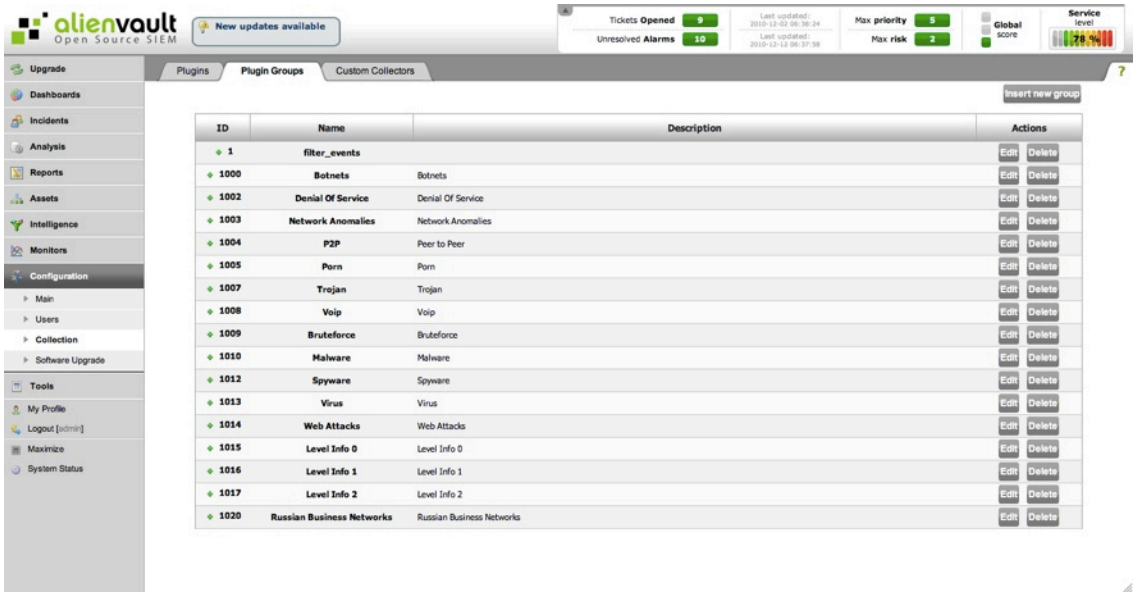
Plugin Groups

Configuration -> Collection -> Plugin Groups

Description

The Plugin Groups page allows you create groups containing event types from the same plugin (Data Source) or even containing events from different plugins.

As an example, you can create a Plugin Group that includes all events that detect a successful authentication in an application or device. This would allow creating a policy that tells the system that successful authentication events (Included in a plugin group) must be stored only in the SIEM when they occur outside normal working hours.



The plugin groups can be used when defining policies as well as during a forensic analysis of information stored in SIEM or Logger

Usage

This page shows a table with all the Plugin Groups defined in AlienVault. The default installation will include some examples of Plugin Groups. Notice that Plugin Groups are not related with Taxonomy, and they will not be updated automatically to include new event types.

Insert New Plugin Group

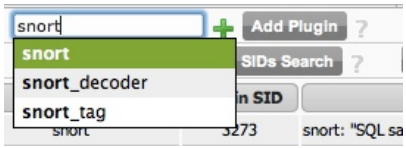
To insert a new Plugin Group simply click on **Insert New Plugin Group** on the top or on the bottom of the table listing all Plugin Groups.

This will show the next screen:

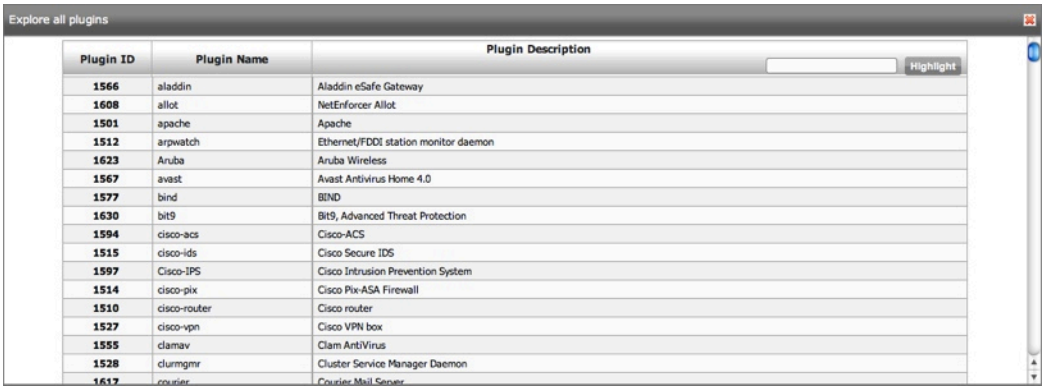
Name and description of the Plugin Group are mandatory fields. Try to use an easy to remember name as you will be able to use this as a search criterion in SIEM and Logger consoles.

Now you must define the types of events that will be part of this Plugin Group. To do this you can select the plugin (Data Source Type) from which you select the events, or search for all types of events that contain a text string in their names.

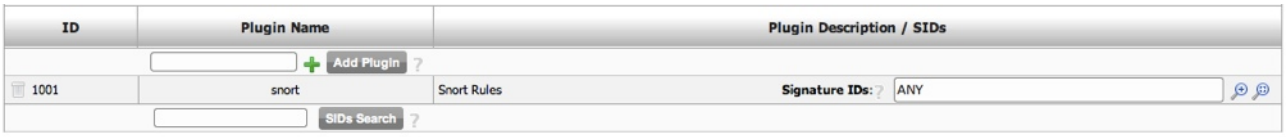
To include even types (Plugin SID) from a particular Data Source Type (Plugin ID) enter the name of the Plugin. The form will help you with auto-completion.



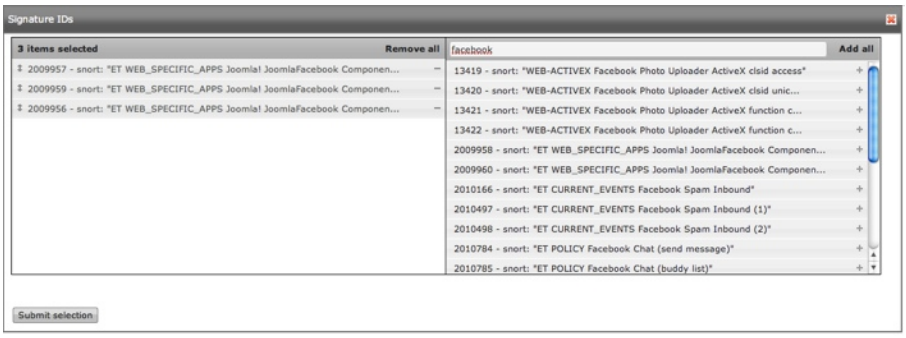
If you do not know the name of the Plugin click on  to display a list of all Plugins.



Simply click on the line of the Plugin you want to select even types from. In the following example we will select events from the Snort Rules plugin (Plugin ID 1001). By default, all events in this plugin will be included in the Plugin Group. You can select only certain events within this plugins by writing the Plugin SIDs in the Signature IDs separated by comma.



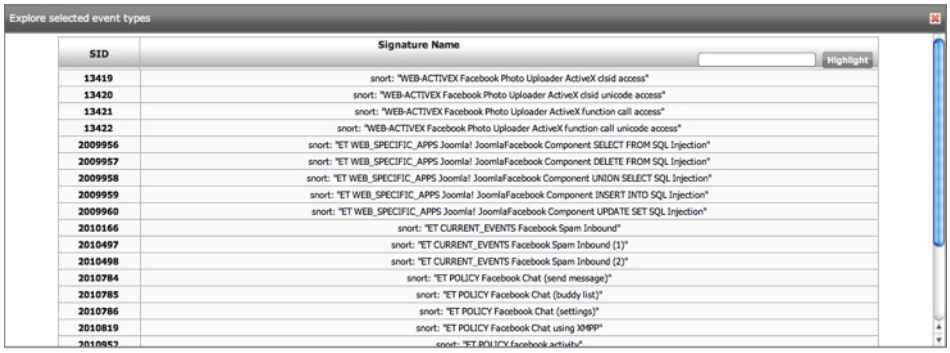
To explore the event types within this Plugin click on . This will show a floating window with two columns. Event types in the left side are events that have already been added to the Plugin Group. Events in the right side can be added to the Plugin group using drag and drop, by moving them to the left side. In the top of the right column you can also search a text string and then click on **Add all** to include all events matching the search criteria in the Plugin Group.



By clicking on **Remove all** you will clean the selection so none of the events within the Plugin will be added to the Plugin Group.

To save changes click on **Submit selection.**

To see the list of events that have already been included in the Plugin Group click on



The same process can be used to include event types from any other Plugin (Data Source Type) in the Plugin Group.

To include all event types from any Plugin matching a search criteria you can use the **SIDs Search**. Enter the text you would like to match in the events name and click on **SIDs Search**.

Then select the Event Types you would like to include in the Plugin Group by marking the checkboxes in each line or mark the checkbox next to the Plugin ID column title to include all event types matching the search criteria. Click on **Add Selected** to save changes.

Edit a Plugin Group

To edit a plugin group, click the **Edit** button in the line that represents the Plugin Group that you wish to edit. Use the process described previously in New Insert Plugin Plugin group to modify the Plugin Group.

Delete a Plugin Group

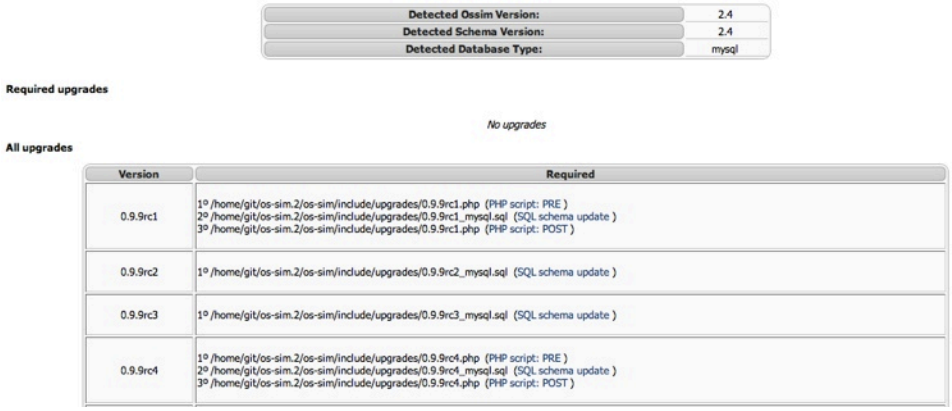
To delete a plugin group, click the **Delete** button in the line that represents the Plugin Group that you wish to delete.

Software Upgrade

Software Upgrade

Configuration -> Software Upgrade -> Software Upgrade

The upgrade process will automatically update the database schema. This section will show a historical of all database upgrades that have been applied.



Detected Ossim Version:	2.4
Detected Schema Version:	2.4
Detected Database Type:	mysql

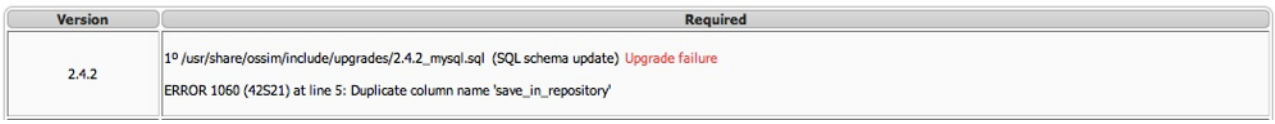
Required upgrades

No upgrades

All upgrades

Version	Required
0.9.9rc1	1º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc1.php (PHP script: PRE) 2º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc1_mysql.sql (SQL schema update) 3º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc1.php (PHP script: POST)
0.9.9rc2	1º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc2_mysql.sql (SQL schema update)
0.9.9rc3	1º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc3_mysql.sql (SQL schema update)
0.9.9rc4	1º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc4.php (PHP script: PRE) 2º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc4_mysql.sql (SQL schema update) 3º /home/git/os-sim.2/os-sim/include/upgrades/0.9.9rc4.php (PHP script: POST)

If the updates have not been done correctly, this section will appear after the user log in. In this case, you will have to apply database updates manually. In case the database cannot be upgraded correctly please report to the AlienVault Support Team.



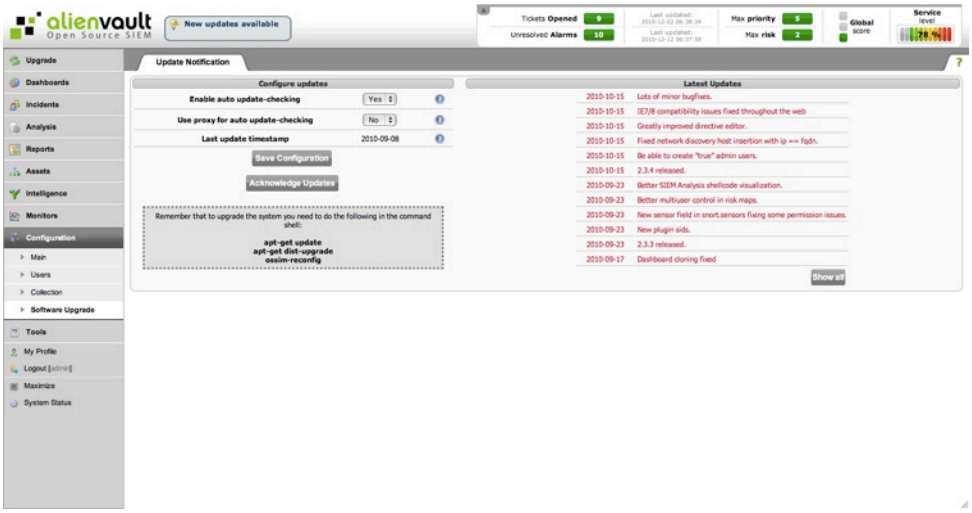
Version	Required
2.4.2	1º /usr/share/ossim/include/upgrades/2.4.2_mysql.sql (SQL schema update) Upgrade failure ERROR 1060 (42S21) at line 5: Duplicate column name 'save_in_repository'

Update Notification

Configuration -> Software Upgrade -> Update Notification

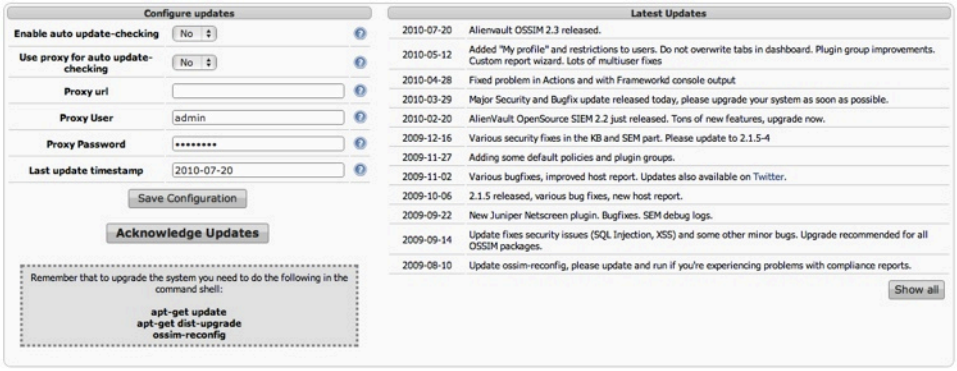
Description

AlienVault can be configured to automatically check the availability of the new software updates.



Usage

If new updates are available a message will be shown in the Top Bar. Clicking on that message will take you to this section, where you will be able to see new features and improvements included in the new software packages. Once you have read that message click on “Acknowledge Updates” to remove the notification message from the top bar.



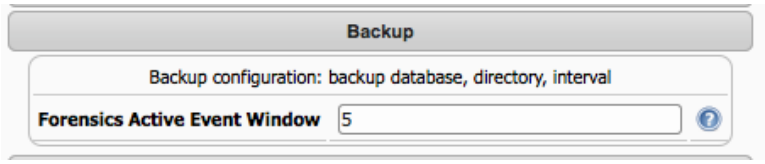
Tools

Backup

Tools -> Backup

Description

Events in the SIEM are purged from the database when they are older than the parameter defined in ***Configuration → Main → Backup*** . The parameter is called **Forensics Active Event Window,** and defines the number of days that will be stored in the forensic database. By default the events of the last 5 days will be kept in the SQL Database.



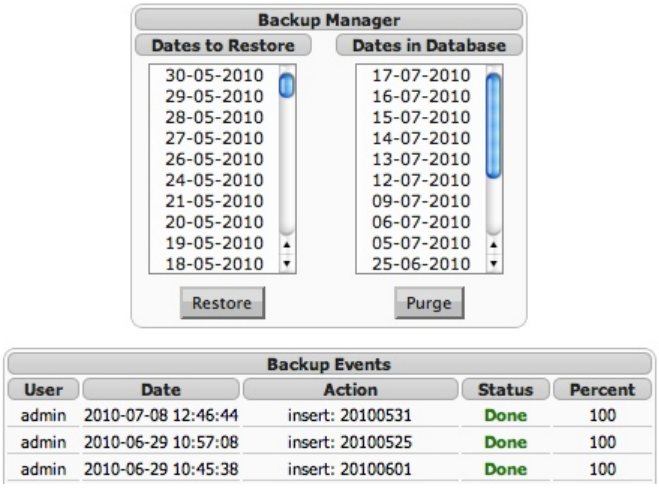
This number can be increased depending on the hardware that is being used and the number of events per day that are been collected and stored when using the SIEM. This parameter only applies to the SIEM, not to the Logger.

If navigating through the AlienVault Web interface takes too long, try decreasing the number of days' worth of events that are kept in the database. On the other hand, if your system is collecting a few events per day, you may want to increase the number of days that are been stored in the database.

Events are never deleted after been purged from the database, they are just stored in a file and they can be restored later on, using the form available in **Tools → Backup**

Usage

Dates that can be restored appear in the Backup Manager, below the dates to restore column. Simply click a date and then click on **Insert**. AlienVault then performs the restoration and displays the status of the restore below in the Backup Events section.



To purge a restored day, click the date of the event in the Dates in Database section and click on **Purge**.

Downloads

Tools -> Downloads

The downloads sections provides links to preconfigured software packages for AlienVault operation. Currently it includes:

- **Putty** : PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is available with source code and is developed and supported by a group of volunteers.
- **AlienVault Agent installer for Windows**: AlienVault Agent installer for windows hosts, server ip is already preconfigured. Run the installer and afterwards go to \AlienVault\ and run 'AlienVault.bat'.
- **Python for Windows** : Python is a remarkably powerful dynamic programming language that is used in a wide variety of application domains. Python is often compared to Tcl, Perl, Ruby, Scheme or Java.
- **OCS** : Open Computer and Software Inventory Next Generation is an application designed to help a network or system administrator keep track of the computers configuration and software that are installed on the network.
- **OSSEC Agent for Windows**: OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response.
- **Snare for Windows**: Snare for Windows is a Windows NT, Windows 2000, Windows XP, Vista and Windows 2003 compatible service that interacts with the underlying Windows Eventlog subsystem to facilitate remote, real-time transfer of event log information.
- **Snare Config file (Audit service takeover)**: Import this .reg file into every host running snare. It's configure to log against this host's IP, you may edit it to change it. This file takes over control of the windows audit service, allowing for easy policy specifications via Snare's web interface. This is the recommended way of running it.
- **Snare Config file (No audit service takeover)**: Import this .reg file into every host running snare. It's configure to log against this host's IP, you may edit it to change it. This file leave's the hosts audit service settings untouched.
- **FW1Loggrabber**: FW1-Loggrabber is a command-line tool to grab log files from Checkpoint FW-1 remotely using Checkpoints LEA (Log Export API), which is one part of Checkpoints OPSEC API.
- **Osiris Windows**: Osiris is a Host Integrity Monitoring System that periodically monitors one or more hosts for change. It maintains detailed logs of changes to the file system, user and group lists, resident kernel modules, and more.

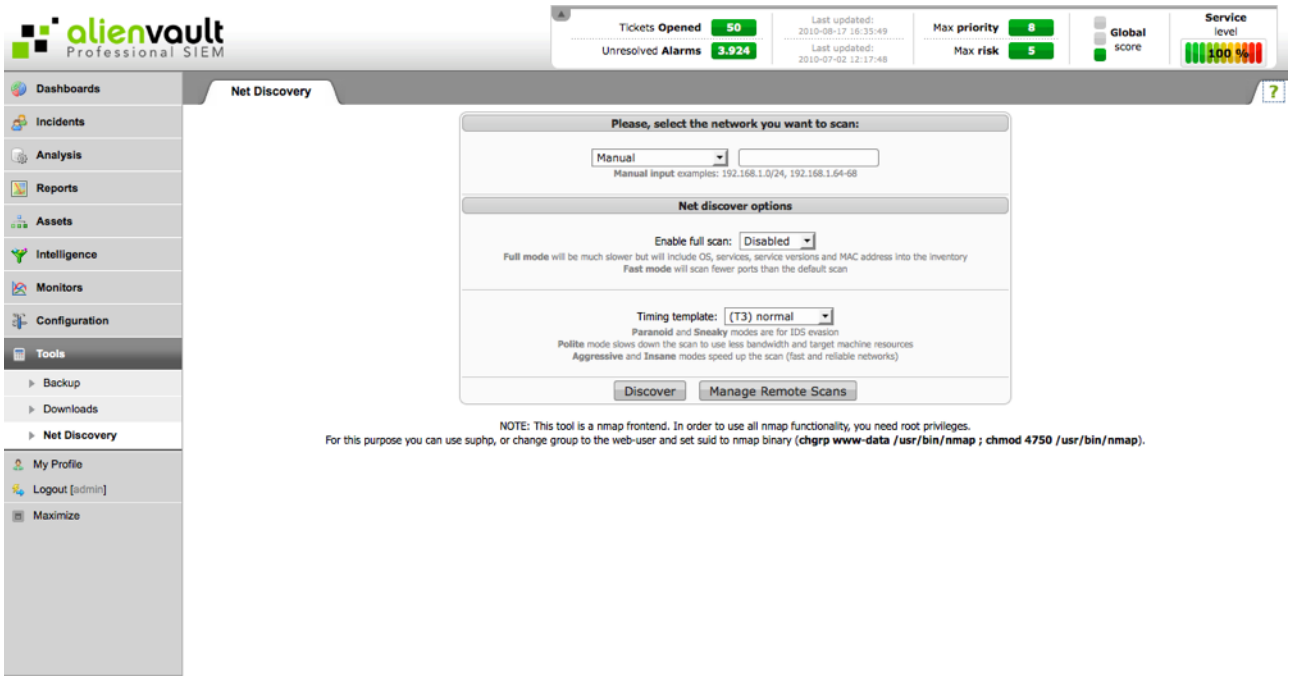
Net Discovery

Tools -> Net Discovery

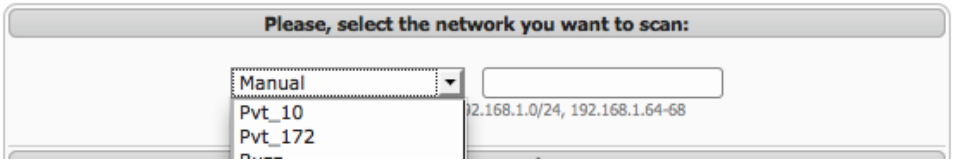
Description

Net Discovery allows scans from the AlienVault system in order to discover assets on the network and to ensure that no changes have occurred in services, operating systems and MAC addresses that use each of the IP addresses of the network.

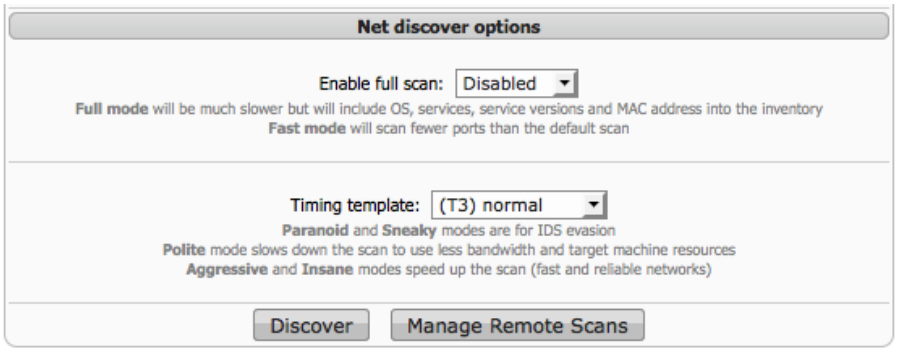
Scanning is done using NMAP in a distributed manner, if the network has an associated sensor in the AlienVault inventory. In case of failure of the distributed scanning, scanning will be done from the machine running the AlienVault Web Interface.



Usage



Using the form above, it is possible to scan for a network asset that we have previously defined in the inventory of AlienVault (***Assets → Network***) or write a network manually for it to be scanned. If you want to add some new network you need to go to ***Assets → Networks*** and define a new one.



When launching the scan you can set the scanning profile that will be used when scanning the network:

- **Full Mode** will be much slower but will include OS, services, service versions and MAC address that can be inserted into the inventory
- **Fast mode** will scan fewer than the default scan

The timing template can also be configured by choosing one of the following:

- Paranoid
- Sneaky
- Polite
- Normal
- Aggressive
- Insane

Paranoid and Sneaky modes are for IDS evasion. Polite mode slows down the scan to use less bandwidth and target machine resources. Aggressive and Insane modes speed up the scan (fast and reliable networks)

Once you are ready, click on Discover. AlienVault scans the network and displays a message once it is complete. The Click here to show the results link appears; the results appear back in the NET Scan page below the select network table.

You can click the Update Database Values, which displays the Insert new scan page. This page allows you to add global properties to the freshly scanned host. These properties are:

- Asset
- Threshold C
- Threshold A
- RRD Profile
- Insert new profile?
- NAT
- Sensors
- Scan options
- Description

Some properties may have corresponding links that allow you to perform additional tasks, especially when working with sensors. Once you have completed any changes, click OK. You can click Reset to return to initial values. To perform the scan, the system makes use of Nmap.

My Profile

My Profile
Description

From this page each user can update their personal information and change the password to access the AlienVault Web Management interface.

Usage

The system can change these settings using a form:

- **User name:** Name of the person associated with the User login
- **User email:** Email address of the user. It will be used to receive information regarding tickets, alarms notifications...
- **User language:** Language for this user in the AlienVault Web Management interface (
- **Company / Department:** Optional fields to identify the role of the user within the corporation that is been monitored.
- **Password:** Password used with the User login.

The option **Ask to change password at next login** will ask the user to change his password after the next successful login.

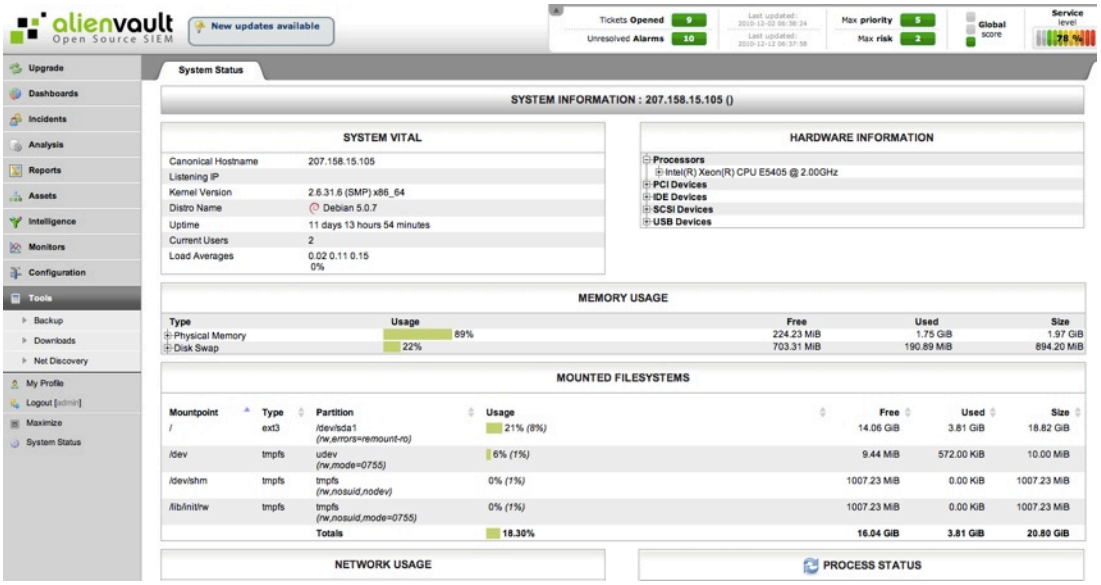
System Status

System Status
Description

This page provides information on the software and hardware being used in the AlienVault appliance.

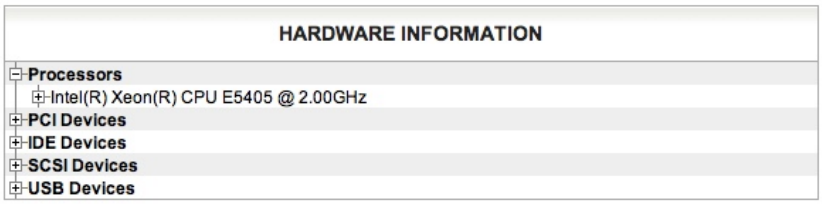
It also allows monitoring the status the system in real-time offering information such as disk space, CPU usage, and memory usage.

To support these requests this page will also display information about the software installed and events extracted from important log files.



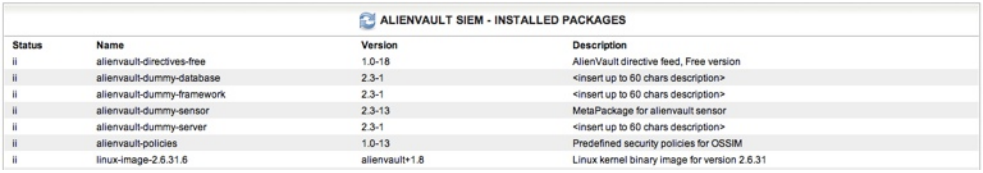
Usage

Part of the information on this page is displayed using trees. For further information click on the **+** in the tree.



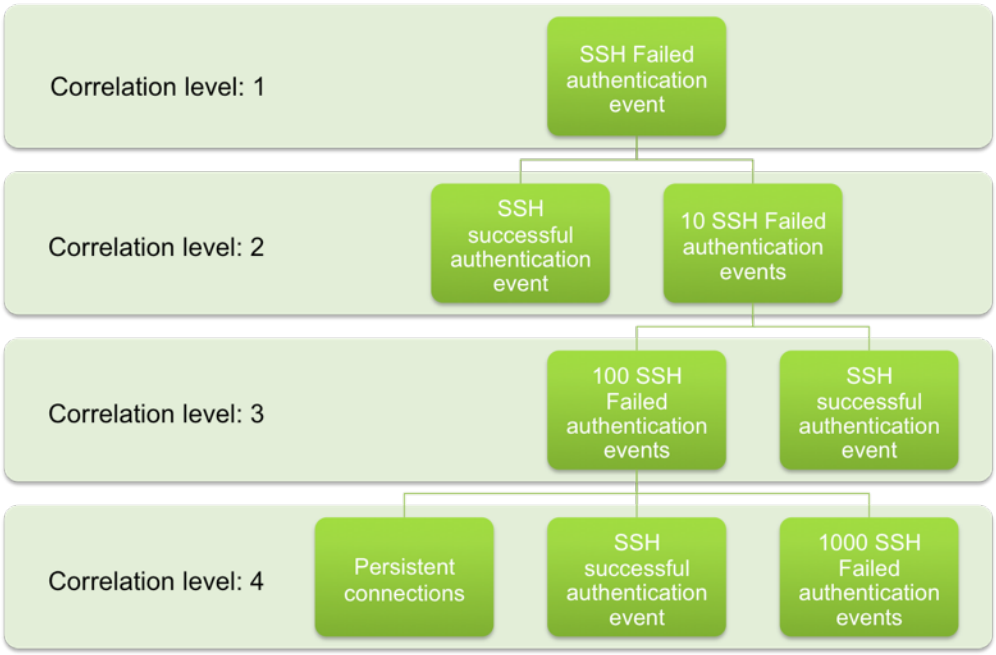
To hide the information, click on the **-** symbol.

Some fields will show real-time information. To update the information displayed click on this icon 



Writing correlation rules

You will learn how to write a correlation directive using the following example. You will try to detect a brute force attack against an SSH Server. As source of information you will mainly use events coming from the SSHD Plugin (Plugin ID: 4003), but we will also use a monitor plugin to check if a connection has been established between the attacker and the machine under attack.



Using correlation rules within the directive you basically define conditions that will be met by the incoming events. Whenever a rule is matched a new event is generated. This event will be processed by the AlienVault Server as if it were coming from a collector. This way you can apply policies to events generated during correlation.

Events generated within the same directive will be grouped into the same alarm.

XML syntax

Directives are written using XML syntax. Because of the way in which information is parsed when using XML files is important to pay attention to theXML syntax, so it is highly recommended to use an XML editor to avoid, as far as possible syntax errors.

Same as when you code HTML, when writing a correlation directive any opened tag should be closed lately.

You can close tags using this syntax: Eg:rule

- Open the rule tag: <rule>
- Close the rule tag: <\rule>

Whenever there is nothing happening inside one of the tags it can also be closed using the backslash at the end of the tag: **\>**

Directive global properties

Each directive will be opened and closed with the directive tag. Within this tag you will have to include the name of the directive, the id of the directive, and the global priority of the directive.

In our example we will give this directive a priority of 4, and we will use an id within the range reserved for user-created directives.

```
<directive id="500000" name="SSH Brute Force Attack Against DST_IP" priori-
ty="4"> </directive>
```

Name

Name Given to the directive. This is the name that will take all the events generated within this directive. You can use the following variable to be replaced by the value of the variable when the alarms are displayed in the Web console (Incidents → Alarms): SRC_IP, DST_IP, SRC_PORT and DST_PORT.

Id

Numeric identifier of the directive, this number must be unique for each directive. The following range is reserved for user-created directives: 500000 - 999999

The events generated during the correlation of each of the directives will take 1505 as plugin_id and the id of the directive as plugin_sid. This way events generated within one of the directives can be used to define a more complex pattern in a different directive.

Priority

When we talk about priority we're talking about threat. It's the importance of the isolated attack. It has nothing to do with your equipment or environment. It only measures the relative importance of the attack. This will become clear using a couple of examples .

- Your unix server running samba gets attacked by the Sasser worm .
  - The attack per se is dangerous, it has compromised thousands of hosts and is very easy to accomplish. But. does it really matter to you? Surely not, but it's a big security hole so it'll have a high priority .

- You're running a CVS server on an isolated network that is only accessible by your friends and has only access to the outside. Some new exploit tested by one of your friends hits it .
  - Again, the attack is dangerous, it could compromise your machine but surely your host is patched against that particular attack and you don't mind being a test-platform for one of your friends .

Priority will be numerical value from 0 up to 5. All events generated within the same directive will have the same directive but they may have a different reliability as it will depend on the correlation level in which the event has been generated.

Correlation level: 1

All events will try to match the first level of every enabled correlation directive once they arrive to the AlienVault Server. This behavior can be modified defining a policy in (Intelligence → Policy & Actions).

The first rule of a directive will have special conditions:

- It will always be a detector rule. Monitor rules can not be used in the first level of directives.
- It will wait for a single occurrence of an event
- It will have no time out. The condition of the first level will last as long as the server is running and the directive enabled
- The event will only be generated for the first directive rule whenever the directive has only one correlation level

In the directive we are creating the correlation will start with any event coming from the SSH Server that refers to an authentication failed attempt. We should always try to cover all possible variants of an attack, in a SSH brute force attack we will find the following events:

- Failed Password
- User blocked
- Root login not allowed
- Illegal user
- User does not exist
- … and much more

So when writing a correlation rule we should always think about all possible events that may be interesting for our new correlation rule. You can take a look to all events that can be generated by each plugin in the following section: Configuration → Collection

Each rule will always wait for events with the same Plugin ID. In this case we will be waiting for events with the Plugin ID 4003, and the following plugin SID which correspond to the type of events we get when we are suffering a brute force attack against one of our SSH Servers:

```
plugin_id="4003"plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
```

So the first rule will be like this:

```
<rule type="detector" name="SSH Authentication failure" reliability="0"
   occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
   plugin_id="4003" plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"/>
```

Notice that I am setting reliability to 0, so the event generated when this correlation rule is matched will never become alarm.

RISK = (Asset Value*Priority*Reliability)/25 RISK = (Asset Value*Priority*0)/25=0

I am also setting occurrence to 1, as the first level of a directive will always collect only 1 event. If we set occurrence field to a higher value the AlienVault Server will automatically set it to 1 when loading the directive.

I am also assuming that the attacker can be inside or outside my monitored network. If I wish to monitor attacks coming from my internal network only I should have placed HOME_NET in the from field.

The directive will now look as follows:

```
<directive id="500000" name="SSH Brute Force Attack Against DST_IP" priori-
ty="4">
      <rule type="detector" name="SSH Authentication failure" reliability="0"
            occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
            plugin_id="4003" plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"/>
</directive>
```

Correlation level: 2

We will reach the second correlation level after getting one of the Authentication Failed Events from one of our SSH Servers. In this correlation level we will have two possibilities:

- Getting almost immediately an authentication successful event (Same source and same destination as the event that matched the first correlation level)
- Getting more authentication failed events (Same source and same destination as the event that matched the first correlation level)

In case we get an authentication successful event the correlation of this directive will be finished. In case we keep getting more authentication failed events then we will reach the third correlation level.

We will also set a time out, as we don not want to wait for so long assuming that a brute force attack will generate a lot of events in a short period of time and not in the next two years. We have also set the reliability value to 1, as we consider that login after only one login failed does not seem to be a brute force attack.

So the first rule of the second correlation level will look as follows:

```
<rule type="detector" name="SSH Successful Authentication (After 1 failed)"
         reliability="1" occurrence="1" from="1:SRC_IP" to="1:DST_IP"
         port_from="ANY" time_out="15" port_to="ANY"
         plugin_id="4003" plugin_sid="7,8"/>
```

This means that once we reach the second correlation level the AlienVault Server will wait for 15 seconds for an authentication successful event with the same source and same destination as the event that matched the previous level.

All rules in the same correlation level will try to collect events at the same time, so the AlienVault server doesn't have to wait for 15 seconds to start the second rule in the second correlation level. We can also have rules with different time_out values. In our case we will wait 40 seconds expecting to collect 10 Authentication Failed events with the same source and same

destination ip addresses that matched the first correlation level. So the first 15 seconds both rules could be matched by the incoming events, but after that only the second rule of the second correlation level will keep alive waiting for incoming events.

In this case, the events matching this rule, would also match the first correlation rule of the directive. That's why we are using **sticky="true"** so we avoid that events getting into this correlation level start their own directive and we keep grouping those events within the same Correlation directive.

```
 <rule type="detector" name="SSH Authentication failure (10 times)"
        reliability="2" occurrence="10" from="1:SRC_IP" to="1:DST_IP"
        port_from="ANY" time_out="40" port_to="ANY"
              plugin_id="4003"  plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
sticky="true"/>
```

We will use the rules tag to open each correlation level (The first one will be started with the directive tag):

```
<rules>
<rule type="detector" name="SSH Successful Authentication (After 1 failed)"
        reliability="1" occurrence="1" from="1:SRC_IP" to="1:DST_IP"
        port_from="ANY" time_out="15" port_to="ANY"
        plugin_id="4003" plugin_sid="7,8"/>
<rule type="detector" name="SSH Authentication failure (10 times)"
        reliability="2" occurrence="10" from="1:SRC_IP" to="1:DST_IP"
        port_from="ANY" time_out="40" port_to="ANY"
           plugin_id="4003"     plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
sticky="true"/>
</rules>
```

Once one of the rules is matched by incoming events, the other rule is discarded and correlation will continue if there are some other rules defined after the rule that has been matched.

Our directive now looks as follows:

```
<directive id="500000" name="SSH Brute Force Attack Against DST_IP" priori-
ty="4">
      <rule type="detector" name="SSH Authentication failure" reliability="0"
            occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
            plugin_id="4003" plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20">
                  <rules>
                        <rule type="detector" name="SSH Successful
                                    Authentication (After 1 failed)"
                              reliability="1" occurrence="1"
                              from="1:SRC_IP" to="1:DST_IP"
                              port_from="ANY" time_out="15" port_to="ANY"
                              plugin_id="4003" plugin_sid="7,8"/>
                        <rule type="detector"
                              name="SSH Authentication failure (10 times)"
                              reliability="2" occurrence="10" from="1:SRC_IP"
                              to="1:DST_IP"
                              port_from="ANY" time_out="40" port_to="ANY"
                              plugin_id="4003"
                              plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
                              sticky="true"/>
                  </rules>

            </rule>
</directive>
```

In this correlation level we may have an alarm generated, as we the event generated in the second rule will have a priority of 4, a reliability of 2 we will have the following risk formula:

RISK = (Asset Value * 4 * 2) /25

An event becomes alarm when it gets a risk higher or equal than 1. So if with a host involved with an asset value of 4 or 5 we would get an alarm after 11 Authentication Failed events (1 of the first correlation level and 10 on the second correlation level)

It is important not to use very high time_out values at a second level of the correlation when the first level of the directive has established simple conditions (plugin_sid="ANY", from="ANY", to="ANY"…) . This will cause many events reaching the second level of correlation, greatly augmenting the memory consumption of the correlation server.

Correlation level: 3

The third correlation level is reached in case you have received a total of 11 SSHD failed authentication events in less than 40 seconds (The first event starts correlation and 10 more will get into the second correlation level).

Here again we have two possibilities, the first will be to collect a successful authentication event, the second option will be waiting to collect more authentication failed events (100).

It is important to note that in case we get the successful authentication event, this will have occurred after several failed attempts so it will be a interesting situation. We will have to increase the reliability in case this rule is matched to ease the generation of an alarm.

The first rule of the third level:

```
<rule type="detector" name="SSH Successful Authentication (After 1 failed)"
      reliability="4" occurrence="1" from="1:SRC_IP" to="1:DST_IP"
      port_from="ANY" time_out="15" port_to="ANY"
      plugin_id="4003" plugin_sid="7,8"/>
```

In case this correlation rule is matched it will generate an alarm when the asset value of one of the host involved is at least 2.

The second rule of the third level:

```
<rule type="detector" name="SSH Authentication failure (100 times)"
      reliability="4" occurrence="100" from="1:SRC_IP" to="1:DST_IP"
      port_from="ANY" time_out="400" port_to="ANY"
      plugin_id="4003"plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
      sticky="true"/>
</rules>
```

Our directive, including the third correlation level will look as follows:

```
<directive id="500000" name="SSH Brute Force Attack Against DST_IP" priority="4">
            <rule type="detector" name="SSH Authentication failure" reliability="0"
                  occurrence="1" from="ANY" to="ANY" port_from="ANY" port_to="ANY"
                  plugin_id="4003" plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20">
                  <rules>
                     <rule type="detector" name="SSH Successful Auth (After 1 failed)"
                            reliability="1" occurrence="1" from="1:SRC_IP" to="1:DST_IP"
                            port_from="ANY" time_out="15" port_to="ANY"
                            plugin_id="4003" plugin_sid="7,8"/>
                       <rule type="detector" name="SSH Auth failure (10 times)"
                            reliability="2" occurrence="10" from="1:SRC_IP"
                           to="1:DST_IP"
                            port_from="ANY" time_out="40" port_to="ANY"
                            plugin_id="4003"
                           plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
                           sticky="true">
                            <rules>
                                <rule type="detector"
                                  name="SSH Successful Auth (After 1 failed)"
                                  reliability="4" occurrence="1"
                                  from="1:SRC_IP" to="1:DST_IP"
                                  port_from="ANY" time_out="100" port_to="ANY"
                                  plugin_id="4003" plugin_sid="7,8"/>
                                <rule type="detector"
                                  name="SSH Auth failure (100 times)"
                                  reliability="4" occurrence="100"
                                  from="1:SRC_IP" to="1:DST_IP"
                                  port_from="ANY" time_out="400" port_to="ANY"
                                  plugin_id="4003"
                                  plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
                                  sticky="true"/>
                            </rules>

                       </rule>
                  </rules>

            </rule>
</directive>
```

Correlation level: 4

On the fourth level of correlation also we will keep open the possibility of keep getting SSH failed authentications or receiving an Authentication successful event. Time_out value will also be increased as well as occurrence a reliability value.

To do that we will use the following two rules:

```
 <rule type="detector" name="SSH Successful Authentication (After 1 failed)"
       reliability="6" occurrence="1" from="1:SRC_IP" to="1:DST_IP"
       port_from="ANY" time_out="150" port_to="ANY"
       plugin_id="4003" plugin_sid="7,8"/>
 <rule type="detector" name="SSH Authentication failure (1000 times)"
       reliability="7" occurrence="10" from="1:SRC_IP" to="1:DST_IP"
       port_from="ANY" time_out="4000" port_to="ANY"
       plugin_id="4003" plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
       sticky="true"/>
```

This level will also include a monitor-type rule, that will be used to check wether is an established established connection between the two hosts (attacker and attacked).

In this case we will use the ntop-session monitor plugin (session-monitor.cfg) . All monitor plugins can be found in the following folder, and they all include monitor in their names:

/etc/AlienVault/agent/plugins/

The ntop is can be queried using the plugin_id 2005, and it supports many different types of request, each request is identified with a different plugin_sid.

In this case we will check the session duration between the two hosts. This request is identified with the plugin_sid 248 and it is defined in the session-monitor.cfg file as follows:

```
[ntop-session-duration]
#192.168.1.42:46378 --> 192.168.1.2:22 (15667.200000 12800.000000) duration: 144

query=/{$from}.html
sid=248
regexp=(?P<ip_src>\d+\.\d+\.\d+\.\d+):(?P<port_src>\d+)\s+-->\s+{$to}:(?P<port_dst>\d+)\s
+\((?P<data_sent>\S+)\s+(?P<data_rcvd>[^\)]+)\)\s+duration:\s+(?P<duration>\d+)
result={$duration}
```

As you can see the monitor plugin is using a variable ($from) to get the information from one of the Ntop webpages, this variable has to be sent by the AlienVault Server request during correlation and it will be used by the monitor plugin to build the query.

So we will build the monitor rule as follows, to check wether there is a connection established for more than 10 seconds:

```
<rule type="monitor" name="More than 10 secs persistence"
         reliability="+4" from="1:SRC_IP" to="1:DST_IP"
         port_from="1:SRC_PORT" port_to="1:DST_PORT" plugin_id="2005"
         plugin_sid="248" condition="ge" value="10" interval="20"
         time_out="120" absolute="true"/>
```

We are sending the source IP, destination IP, Source port and Destination port of the event that matched the previous correlation level. The monitor plugin will be requesting this information to Ntop every 20 seconds (interval) for 120 seconds (time_out). Whenever the condition defined by condition and value is matched (In this case session established for 10 or more seconds), the rule will have been matched and an event will be sent to the AlienVault Server to continue correlating the directive. In our directive correlation will have finished.

The third level will look as follows, same as when using only detector rules, the three rules will be processed at the same time, and whenever one of them is matched the AlienVault server will discard the two other rules.

```
<rule type="detector" name="SSH Successful Authentication (After 1 failed)"
      reliability="6" occurrence="1" from="1:SRC_IP" to="1:DST_IP"
      port_from="ANY" time_out="150" port_to="ANY"
      plugin_id="4003" plugin_sid="7,8"/>
<rule type="detector" name="SSH Authentication failure (1000 times)"
      reliability="7" occurrence="10" from="1:SRC_IP" to="1:DST_IP"
      port_from="ANY" time_out="4000" port_to="ANY"
      plugin_id="4003"
      plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20" sticky="true"/>
<rule type="monitor" name="More than 10 secs persistence"
      reliability="+4" from="1:SRC_IP" to="1:DST_IP"
      port_from="1:SRC_PORT" port_to="1:DST_PORT" plugin_id="2005"
      plugin_sid="248" condition="ge" value="10" interval="20"
      time_out="120" absolute="true"/>
```

Each correlation directive can include as much rules as needed. It is always advisable to include a last level to capture a large number of events. Thus, if the attack continues for a long period of time, these events will be entering into the same directive and grouped within the same alarm.

```
<directive id="500000" name="SSH Brute Force Attack Against DST_IP"
priority="4">
            <rule type="detector" name="SSH Authentication failure"
                  reliability="0" occurrence="1" from="ANY" to="ANY"
                  port_from="ANY" port_to="ANY"
                  plugin_id="4003"
                  plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20">
                  <rules>
                        <rule type="detector"
                              name="SSH Successful Authe (After 1 failed)"
                              reliability="1" occurrence="1" from="1:SRC_IP"
                              to="1:DST_IP"
                              port_from="ANY" time_out="15" port_to="ANY"
                              plugin_id="4003" plugin_sid="7,8"/>
                        <rule type="detector" name="SSH Auth failure (10 times)"
                              reliability="2" occurrence="10"
                              from="1:SRC_IP" to="1:DST_IP"
                              port_from="ANY" time_out="40" port_to="ANY"
                              plugin_id="4003"
                              plugin_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20"
                              sticky="true">
                              <rules>
                                  <rule type="detector"
                                        name="SSH Suc. Auth (After 1 failed)"
                                        reliability="4" occurrence="1"
                                        from="1:SRC_IP" to="1:DST_IP"
                                        port_from="ANY" time_out="100"
                                        port_to="ANY"
                                        plugin_id="4003" plugin_sid="7,8"/>
                                  <rule type="detector" name="SSH Auth f.(100
times)"
                                        reliability="4" occurrence="100"
                                        from="1:SRC_IP" to="1:DST_IP"
                                        port_from="ANY" time_out="400"
                                        port_to="ANY"
                                        plugin_id="4003"
                                        plugin_sid="1,2,3,4,5,6,9,10,12
,13,14,15,16,20" sticky="true">
                                        <rules>
                                              <rule type="detector"
                                                    name="SSH Successful
Authentication (After 1 failed)"
                                                    reliability="6" occur-
rence="1" from="1:SRC_IP" to="1:DST_IP"
                                                    port_from="ANY" ti-
me_out="150" port_to="ANY"
                                                    plugin_id="4003"
plugin_sid="7,8"/>
                                              <rule type="detector" name="SSH
Authentication failure (1000 times)"
                                                    reliability="7" occur-
rence="10" from="1:SRC_IP" to="1:DST_IP"
```

```
                                                        port_from="ANY" ti-
me_out="4000" port_to="ANY"
                                                        plugin_id="4003" plug-
in_sid="1,2,3,4,5,6,9,10,12,13,14,15,16,20" sticky="true"/>
                                                    <rule type="monitor" name="More
than 10 secs persistence"
                                                        reliability="+4"
from="1:SRC_IP" to="1:DST_IP"
                                                        port_from="1:SRC_PORT"
port_to="1:DST_PORT" plugin_id="2005"
                                                        plugin_sid="248" condi-
tion="ge" value="10" interval="20"
                                                        time_out="120"
absolute="true"/>
                                            </rules>
                                    <rule>
                                </rules>
                            </rule>
                        </rules>

                </rule>
</directive>
```

Detector Rule elements

type

What type of rule is this. There are two possible types as of today :

- monitor
- detector

As we are talking about detector rule elements. Type will take detector as value. Eg: type="detector"

name

The name of the rule describes what the system expects to collect in order to satisfy the condition of the rule for the correlation. This name Eg: name="100SSH Auth Failed events"

reliability

Reliability value of every event generated within the directive. It can be an absolute value 0-10 or incremental +2, +6. When using an incremental value, this will be added to the value that has taken the reliability field in the last event generated within this directive.

By assigning the value of reliability for each of the rules is important to remember the formula for calculating the risk in AlienVault. Using high-reliability values at the lowest levels of correlation will get a large number of alarms even when low-valued assets is involved.

Eg: reliability="3" reliability="+3"

occurrence

Number of events matching the conditions given in the rule that have to be collected before the directive generates an event. The first level doesn't have an occurrences value as it will always be one.

time_out

Waiting time before the rule expires and the directive process defined in that rule is discarded. The first rule doesn't have a time_out value.

from

Source IP. There are various possible values for this field :

- **ANY**: Just that, any ip address would match .
- Dotted numerical Ipv4 (x.x.x.x): Self explaining .
- Comma separated Ipv4 addresses without netmask
- Network Name: You can use any network name defined via web (Assets → Networks) .
- **Relative value**: This is used to reference ip addresses from previous levels. This should be easier to understand using examples
  - 1:SRC_IP means use the source ip that matched the condition defined by the previous rule as source ip address.
  - 2:DST_IP means use the destination ip that matched the condition defined two rules below as destination ip address .
- **Negated elements**: You can also use negated elements. I.e. : "!192.168.2.203,INTERNAL_NETWORK".
- If INTERNAL_NETWORK == 192.168.2.0/24 this would match the whole class C except 192.168.2.203.
- **HOME_NET**: This will match only when the Source IP belongs to your Assets, this means that is has been included in the AlienVault inventory as a host or that it belongs to a network or network group that is within your inventory.

to

Destination IP. There are various possible values for this field:

- **ANY**: Just that, any ip address would match .
- Dotted numerical Ipv4 (x.x.x.x): Self explaining .
- Comma separated Ipv4 addresses without netmask
- Network Name: You can use any network name defined via web (Assets → Networks) .
- **Relative value**: This is used to reference ip addresses from previous levels. This should be easier to understand using examples
  - 1:SRC_IP means use the source ip that matched the condition defined by the previous rule as source ip address.
  - 2:DST_IP means use the destination ip that matched the condition defined two rules below as destination ip address .
- **Negated elements**: You can also use negated elements. I.e. : "!192.168.2.203,INTERNAL_NETWORK". If INTERNAL_NETWORK == 192.168.2.0/24 this would match the whole class C except 192.168.2.203.
- **HOME_NET**: This will match only when the Source IP belongs to your Assets, this means that is has been included in the AlienVault inventory as a host or that it belongs to a network or network group that is within your inventory.

sensor

- **ANY**: Just that, any AlienVault Sensor would match .
- Dotted numerical Ipv4 (x.x.x.x): Self explaining .
- Comma separated Ipv4 addresses without netmask
- **Sensor Name**: You can use any Sensor name defined via web (Assets → SIEM Components → Sensors) .
- **Relative value**: This is used to reference ip addresses from previous levels. This should be easier to understand using examples
- 1:SENSOR means use the Sensor that matched the condition defined by the previous rule
- **Negated elements**: You can also use negated elements, separated by comma. I.e. : "!192.168.2.203,ANY".

port_to

This can be a port number or a sequence of comma separated port numbers. ANY port can also be used. Hint: 1:DST_PORT or 1:SRC_PORT would mean level 1 src and dest port respectively. They can be used too. (level 2 would be 2:DST_PORT for example).

Also you can negate ports. This will negate ports 22 and 21 in the directive:

port="!22,25,110,!21"

port_from

This can be a port number or a sequence of comma separated port numbers. ANY port can also be used. Hint: 1:DST_PORT or 1:SRC_PORT would mean level 1 src and dest port respectively. They can be used too. (level 2 would be 2:DST_PORT for example).

Also you can negate ports. This will negate ports 22 and 21 in the directive:

port="!22,25,110,!21"

protocol

This can be one of the following strings:

- TCP
- UDP
- ICMP
- Host_ARP_Event
- Host_OS_Event
- Host_Service_Event
- Host_IDS_Event
- Information_Event

Additionally, you can put just a number with the protocol.

Although Host_ARP_Event, Host_OS_Event, etc, are not really a protocol, you can use them if you want to do directives with ARP, OS, IDS or Service events. You can also use relative referencing like in 1:TCP, 2:Host_ARP_Event, etc…

You can negate the protocol also like this: protocol="!Host_ARP_Event,UDP,!ICMP" This will negate Host_ARP_Event and ICMP, but will match with UDP.

plugin_id

Numerical identifier of the tool that provides the information (Events in detector rules and indicators in monitor rules)

plugin_sid

Numerical identifier of the type of event within the tool defined by plugin_id that must met the condition defined by the directive rule. plugin_sid can take ANY as value, or a relative value when it is being used in a second or higher correlation level: Eg plugin_sid="1:PLUGIN_SID"

sticky

When the events arrive to the correlation engine they will try to be correlated inside directives whose correlation has been started

Using sticky we avoid those events to start the correlation of the same directive again, as they may also meet the conditions given by the same directive. Eg: sticky="true" or sticky="false"

sticky_different

This variable can be associated to any field in rules with more than one occurrence, to make all the occurrences have a different value in one of the fields.

Eg: sticky_different="DST_PORT" (All the events matching the rule must have a different destination port (Port scanning detection))

Username, password, filename, userdata1, userdata2, userdata3, userdata4, userdata5, userdata6, userdata7, userdata8, userdata9

This keywords are optional. They can be used to store special data from agents. Obviously, this only will work if the event has this fields. The following values are accepted: You can insert any string to match here. If you want that this matches with any keyword, you can skip these keywords, or use ANY as the value.

- **ANY**: Just that, this will match with any word. You can also avoid this keyword, and it will match too.
- **Comma separated list**:You can use any number of words separated by commas
- **Relative value**: This is used to reference keywords from previous levels, for example:
- 1:FILENAME → Means use the filename referenced in the first rule level
- 2:USERDATA5 → Means use some data from USERDATA5 keyword referenced in the second rule level
- **Negated**: You can also use negated keywords, i.e: "!johndoe,foobar". This will match with foobar, but not johndoe
    - Here you can see an example of what can be done:
    - username="one,two,three,!four4444,five" filename="1:FILENAME,/etc/password,!/etc/shadow" userdata5="el cocherito lere me dijo anoche lere,!2:USERDATA5"

NOTE: There are some special events that have extra fields:

- Arpwatch events: Userdata1 = MAC
- Pads events: Userdata1 = application ; Userdata2 = service
- P0f Events: Userdata1 = O.S.
- Syslog Events: Username = dest username ; Userdata1 = src username ; Userdata2 = src user uid ; Userdata3 = service

Monitor Rule elements

type

What type of rule is this. There are two possible types as of today :

- monitor
- detector

As we are talking about monitor rule elements. Type will take monitor as value. Eg: type="monitor"

name

The rule name should describe the type of information that we obtain when querying the tool or device during correlation using the monitor plugin.

reliability

Reliability value of every event generated within the directive. It can be an absolute value 0-10 or incremental +2, +6. When using an incremental value, this will be added to the value that has taken the reliability field in the last event generated within this directive.

By assigning the value of reliability for each of the rules is important to remember the formula for calculating the risk in AlienVault. Using high-reliability values at the lowest levels of correlation will get a large number of alarms even when low-valued assets is involved.

Eg: reliability="3" reliability="+3"

plugin_id

Numerical identifier of the monitor plugin that will query the device or application to feed the correlation engine with indicators while correlation takes place.

plugin_sid

Numerical identifier of the request or query that has to be executed. In this case we can not use ANY or a relative value.

time_out

Waiting time before the rule expires and the directive process defined in that rule is discarded. The first rule doesn't have a time_out value.

condition

The condition field establishes a logical relation between the value field and the value returned in the monitor plugin request. It can take the following values:

eq equal

ne non equal

lt less than

gt greater than

le less or equal

ge greater or equal

value

This field sets the value that has to be compared with the value returned by the collector after doing the monitor request.

Value must be an integer. Eg: value="333"

time_out

Waiting time before the rule expires and the directive process defined in that rule is discarded.

interval

This value of this field sets the waiting time between each monitor request before the rule is discarded because the time defined by time_out is over.

absolute

This value sets if the value that has to be compared is relative or absolute.

Absolute true: If the host has more than 1000 bytes sent during the next 60 seconds. There will be an answer if in 60 seconds this value is reached. absolute="true"

Absolute false: If the host shows an increase of more than 1000 bytes sent. There will be an answer if the host shows this increase in 60 seconds. absolute="false"

from, to, port_from, port, to, protocol, sensor,Username, password, filename, userdata1, userdata2, userdata3, userdata4, userdata5, userdata6, userdata7, userdata8, userdata9

In monitor type rules, these fields are not used to define a condition that must be matched by the events arriving to the the AlienVault server. These fields will be used to send information to the collector in order to be used in the query that is done through a monitor plugin.

For this reason it does **not** makes sense to use values such as HOME_NET or ANY. You will need to write the value that has to be send to the build the query of the monitor plugin: Eg: from="192.168.2.2" or use a relative value such as from="1:SRC_IP" to send to the monitor plugin the ip address that matched as source ip in the previous correlation level.

Further reading and Information

Reporting Bugs

Reporting a bug with all required information will reduce the time required by the developer to fix it. When reporting a bug keep this in mind:

- Be precise
- Be clear
- Report every possible bugs, as small bugs may hide bigger bugs
- Read the documentation to make sure it is not the expected behavior
- Read what you wrote

You should always make sure that your are using the latest version available before filling the Bug Report. It will also be very helpful if you were including hardware information and a quick note about how is your deployment: Eg: Server only in one box and three remote Sensors).

Bugs must be filled in in the following Web Site: https://www.assembla.com/spaces/os-sim/support/tickets

AlienVault

Website

The website http://www.AlienVault.com contains information of AlienVault, the company, as well as information about the AlienVault product, in both Professional and Open Source edition.

Forums

AlienVault forums are the perfect place to exchange experiences with AlienVault user community.

AlienVault forums can be accessed using the following URL: https://www.AlienVault.com/forum/

IRC

The AlienVault IRC channel is a dedicated chat room ideal for getting real-time help from other users community users. The channel name is #AlienVault on irc.freenode.net