



USM Appliance™

User Guide

Copyright © 2023 AT&T Intellectual Property. All rights reserved.

AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or affiliated companies. All other marks are the property of their respective owners.

Updated September 27, 2023

Contents

Introduction to USM Appliance	8
Prerequisites and Requirements	10
USM Appliance Network Security Concepts and Terminology	11
About USM Appliance Components	12
About USM Appliance Network Security Capabilities	13
The USM Appliance Web User Interface	15
Getting Started with USM Appliance	20
USM Appliance Network Security Best Practices	21
What Expectations Should I Have of Security Monitoring?	22
USM Appliance Event Processing Workflow	22
Verifying USM Appliance Operation	24
Establishing Baseline Network Behavior	30
USM Appliance Security Monitoring and Analysis	34
USM Appliance Dashboards	35
Analyzing Alarms, Events, Logs, and Tickets	41
Managing the USM Appliance Environment	48
USM Appliance Administration and Configuration	59
Asset Management	69
Assets and Groups	71
Adding Assets	74
Asset Administration	86
Asset Group Administration	108
Network Administration	114
Network Group Administration	118
Alarm Management	120
Alarms Page Overview	121

Reviewing Alarms as a Group	122
Reviewing Alarms as a List	124
Taking Ownership of an Alarm	136
Back Up and Restore Alarms	138
Event Management	142
Events Page Overview	143
USM Appliance Event Taxonomy	144
Review Security Events	149
Back Up and Restore Events	169
Clear All Events from the SIEM Database	173
Event Storage Best Practices	174
Network Data Management	177
NetFlow Monitoring	178
NetFlow Monitoring Configuration	179
NetFlow Event Controls	189
NetFlow Troubleshooting	190
Back Up and Restore NetFlow Data	195
Capture and Examine Packets	198
Raw Log Management	201
Raw Logs Page Overview	202
Graphs and Charts for Raw Logs	203
Search Raw Logs	205
Review and Verify Raw Logs	209
Configure the Digital Signing of Raw Logs	211
Export Raw Logs	213
Back Up and Restore Raw Logs	214
Ticket Management	218
Tickets Page Overview	219

Create a Ticket	219
Search and Close Tickets	222
Edit a Ticket	224
Correlation and Cross-Correlation	227
Event Correlation	228
Correlation Contexts	230
Correlation Directives	230
Tutorial: Create a New Directive to Detect DoS Attack	242
Tutorial: Modifying a Built-In Directive	249
Cross-Correlation	253
Policy Management	258
Use of Policies in USM Appliance	259
Create or Modify a Policy	268
Policy Order and Grouping	286
Tutorial: Create a Policy to Discard Events	288
Tutorial: Create a Policy to Send Emails Triggered by Events	291
Tutorial: Create a Policy to Send Emails for Account Lockout Events	295
Vulnerability Assessment	301
What Is Vulnerability Assessment?	302
Vulnerability Assessment in USM Appliance	302
Vulnerability Risk Factors	302
Vulnerability Scans	303
Viewing the Scan Results	328
Vulnerability Scan Profiles	340
Open Threat Exchange® and USM Appliance	355
What is Open Threat Exchange®?	356
Using OTX in USM Appliance	359
Incident Response	367

What Defines an Incident?	368
What Defines a Breach?	368
What to Include in Your Incident Remediation Plan	368
Developing an Effective Triage Strategy	369
How Do I Discover a Possibly Larger Attack in Progress?	369
USM Appliance Reports	375
About USM Appliance Reports	376
How to Run Reports	377
Create Custom Reports	382
Create Custom Reports from SIEM Events or Raw Logs	385
List of USM Appliance Reports	387
User Administration	399
User Administration in USM Appliance	400
USM Appliance User Accounts	401
User Authentication	402
User Authorization	408
Manage User Accounts	418
Monitor User Activities	428
Using USM Appliance for PCI Compliance	432
PCI DSS 3.2 Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data	434
PCI DSS 3.2 Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters	435
PCI DSS 3.2 Requirement 3: Protect Stored Cardholder Data	447
PCI DSS 3.2 Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks	448
PCI DSS 3.2 Requirement 5: Protect All Systems Against Malware and Regularly Update Anti-Virus Software or Programs	452
PCI DSS 3.2 Requirement 6: Develop and Maintain Secure Systems and Applications	455

PCI DSS 3.2 Requirement 7: Restrict Access to Cardholder Data by Business Need to Know	457
PCI DSS 3.2 Requirement 8: Identify and Authenticate Access to System Components	458
PCI DSS 3.2 Requirement 9: Restrict Physical Access to Cardholder Data	460
PCI DSS 3.2 Requirement 10: Track and Monitor Access to All Network Resources and Cardholder Data	462
PCI DSS 3.2 Requirement 11: Regularly Test Security Systems and Processes	463

Introduction to USM Appliance

This guide provides information for users of the AlienVaultUSM Appliance system, that are responsible for monitoring network security, and identifying and addressing security threats in their environment. The guide also describes operations provided by the USM Appliance web UI, which is used to perform most USM Appliance network security tasks after initial USM Appliance system deployment.

Topics covered in this guide include

- Introduction — this section, which includes
 - [Prerequisites and Requirements](#) — target audience, recommended skills and background, and supported browsers for using the USM Appliance web user interface to perform network security operations.
 - [USM Appliance Network Security Concepts and Terminology](#) — description of key terms such as assets, threats, and vulnerabilities, and how USM Appliance calculates risk for specific assets.
 - [About USM Appliance Components](#) — high-level description of key USM Appliance components: USM Appliance Server, USM Appliance Sensor, and USM Appliance Logger.
 - [About USM Appliance Network Security Capabilities](#) — description of essential USM Appliance security capabilities including asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring and security information and event management (SIEM).
 - [The USM Appliance Web User Interface](#) — description of key elements and navigation of the USM Appliance web user interface (UI) used to access and perform USM Appliance network security monitoring and analysis operations.
- [Getting Started with USM Appliance](#) — details typical security operations performed after initial USM Appliance installation and configuration, including security operation best practices and workflow, verifying USM Appliance operations, and establishing baseline network behavior.
- [USM Appliance Security Monitoring and Analysis](#) — provides an overview of USM Appliance web UI main menu and submenu options and operations used for display, monitoring, and analysis of network security activities and events.

- [Incident Response](#) — provides information on basic elements of incident response, effectively responding to threats ranging from single events or incidents to larger scale attacks involving multi-stage attacks.
- [Asset Management](#) — describes operations to manage assets, asset groups, and asset-based security controls. Covers topics such as asset creation and discovery, vulnerability scans, HIDS deployment, and asset monitoring and analysis.
- [Alarm Management](#) — provides information about alarms generated from events and OTX pulses, viewing and reviewing alarm information and field details, and assigning alarms for remediation with tickets.
- [Event Management](#) — provides information on viewing, filtering, sorting, and analyzing events, alarms, and OTX field details.
- [Network Data Management](#) — describes methods of capturing packet information from network traffic, and NetFlow data providing information about communication between network devices, to supplement information provided by system events and alarms.
- [Raw Log Management](#) — provides information on searching and reviewing raw log information, configuring digital signing and verifying the integrity of raw logs, and exporting raw logs.
- [Ticket Management](#) — details opening, searching, and editing of remediation tickets created using USM Appliance's own ticket management system.
- [Policy Management](#) — provides information on creating and managing policies, defining policy conditions, consequences, and actions.
- [Event Correlation](#) — describes how USM Appliance correlation works and provides information on creating and editing correlation directives or rules.
- [Vulnerability Assessment](#) — Provides information on performing vulnerability scans, viewing and understanding scan results, and generating reports based on vulnerability scans.
- [Open Threat Exchange® and USM Appliance \(OTX\)](#) — describes the open threat data platform allowing security researchers, and the OTX community at large, to share information about the latest threats and evidence of exploit or malicious acts that threaten network security.
- [About USM Appliance Reports](#) — provides information on report categories, creating and customizing reports, and generating reports based on vulnerability scan results.
- [User Administration in USM Appliance](#) — describes USM Appliance user authentication and role-based authorization, configuration of authorization for specific assets, and monitoring user activity.

- [Using USM Appliance for PCI Compliance](#) — provides information on USM Appliance capabilities to validate and document compliance with specific PCI DSS regulations.

Prerequisites and Requirements

The information in this guide is primarily intended for security engineers, security analysts and operators, IT managers and professionals, and system administrators, using USM Appliance to provide network security within their own organization's environment. Users must also have knowledge of their organization's network infrastructure and the networking technologies they use.

Recommended skills for users include the following:

- Basic TCP/IP networking knowledge and skills including IP addressing, DNS, switching, and routing.
- Basic familiarity with IT security concepts and associated skills, including threats, vulnerabilities, risk management and security devices/applications.
- Basic Linux skills, including the use of the command line interface for file and user management, and text editing (using tools such as vi/vim and nano).

Information provided in this guide assumes a customer has completed installation and configuration of AlienVault USM Appliance as described in the Initial Setup section of the *USM Appliance Deployment Guide*. In addition, users of this guide need the appropriate credentials to access USM Appliance, a web browser (to access the USM Appliance web UI through HTTPS), and SSH access (for operations performed from the USM Appliance command line).

USM Appliance supports the following browsers.

Supported Browsers

Browser/Platform	Windows	Mac OS X	Linux
Chrome	Yes	Yes	Yes
Edge	Yes	N/A	N/A
Firefox	Yes	Yes	Yes
Internet Explorer 11	Yes	N/A	N/A
Safari	N/A	Yes	N/A



Note: All USM Appliance releases are tested on the most recent version of the browsers and one version prior to the most recent.

USM Appliance Network Security Concepts and Terminology

When working with USM Appliance and using the USM Appliance web UI to perform network security operations, it is important to understand a few basic USM Appliance network security concepts.

Assets

First, a key tenet of the USM Appliance system is that it monitors assets. Assets are all devices in an enterprise that have some value to the enterprise and, generally, that it is possible to monitor or gather information about, such as their status, health or availability, configuration, activity, and events. The value comprises either the cost of the device itself, or the value of the data that is stored on the device or travels through the device.

- An asset is defined as a unique IP address.
- Assets are organized into networks based on IP addressing.
- Networks are organized into locations or regions, based on their geographical location.

Typically, at least one USM Appliance Sensor is used to monitor one geographically self-contained location. If several locations are used by an enterprise, each location is monitored with at least one USM Appliance Sensor, which sends information to the USM Appliance Server about assets that are in the same location. Plugins are used in the USM Appliance Sensor to extract and normalize data from different data sources into standard-format events. USM Appliance provides a wide assortment of plugins that can be used to collect events for most commonly encountered data sources. You can enable up to 10 plugins per asset and up to 100 plugins per USM Appliance Sensor.

Risk

Another important concept to understand is risk. In most organizations, priorities for network security operations are determined primarily by risk, that is, factors such as the value of assets, the potential damage that particular threats pose to assets and the vulnerabilities those assets have to threats, and the likelihood that actual attacks will be carried out. In USM Appliance, risk values are calculated for each raw event received from the

USM Appliance sensor as well as for additional security events generated as a result of correlation or cross-correlation of multiple events. USM Appliance generates an alarm for any event that has a calculated risk value greater than or equal to 1.

The formula that USM Appliance uses to calculate risk for individual events is the following:

$$\text{Calculated Risk Value} = (\text{Asset Value} * \text{Event Priority} * \text{Event Reliability}) / 25$$

In this formula, *Asset Value* is the value (0 to 5) that your organization assigns to a specific asset that is connected to an event. *Event Priority* is a priority ranking (0 to 5) that is based on the event type, such as authentication failure, web attack, or denial of service, which indicates the urgency with which an event should be investigated. (AlienVault provides an event taxonomy to classify various events by category and subcategory. See [USM Appliance Event Taxonomy](#)). *Event Reliability* is a reliability ranking (0 to 10) that specifies the likelihood that an event is a real attack or a false positive event.

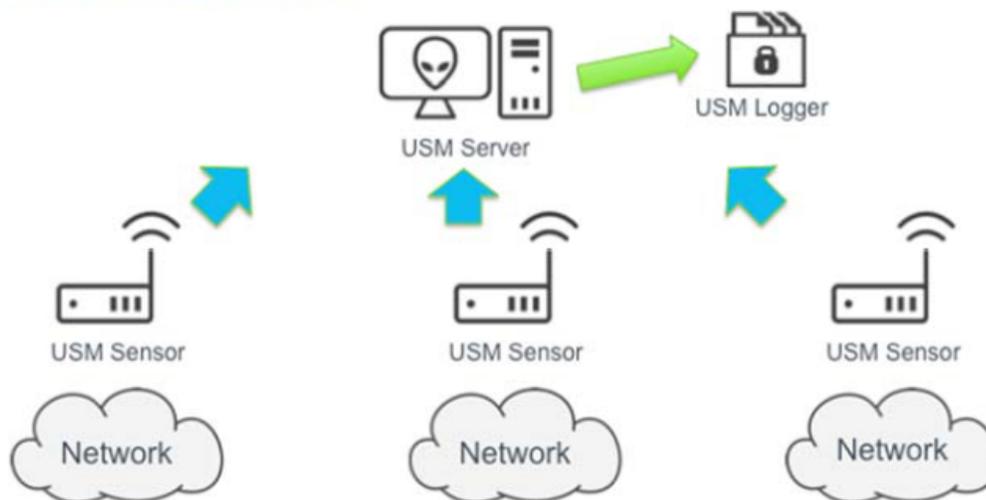
Threats

Finally, threats and vulnerabilities are what correlate the occurrence of certain events with risk and generate alarms when the risk values of events exceed a specific threshold value (greater than or equal to 1). Information about specific threats is obtained from sources such as those reported by AT&T Alien Labs™ and the AT&T Alien Labs™ Open Threat Exchange® (OTX™). For example, OTX provides indicators of compromise and notifications of malicious hosts, which can link assets by their vulnerabilities to specific threats and notification about events that involve known or suspect malicious hosts. (See the [AlienVault OTX User Guide](#) for more information on using OTX.) USM Appliance can also perform scans which identify assets' vulnerabilities to specific, identified threats.

About USM Appliance Components

The following diagram provides a high-level view of the overall USM Appliance architecture.

USM Architecture



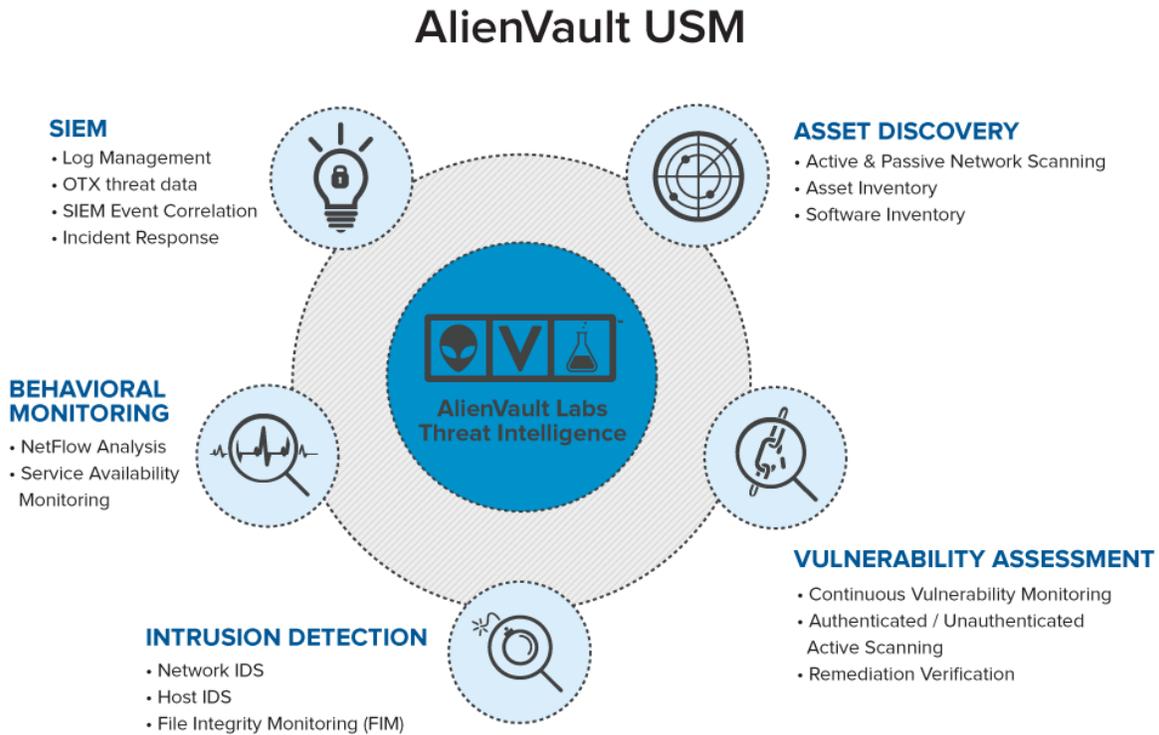
AlienVault USM Appliance has three core components:

- USM Appliance Sensor — deployed throughout your network to collect events from various devices on the network.
- USM Appliance Server — aggregates and correlates information gathered by the USM Appliance Sensors, and provides single pane-of-glass management, reporting, and administration.
- USM Appliance Logger — securely archives raw event log data for forensic investigations and compliance mandates.

The USM Appliance Sensor collects raw log data and other information from various network devices, host servers, and applications, normalizes the data into a standard-event format, and sends the events on to the USM Appliance Server. Customers can choose from over 200 sensor plugins to process raw log files and other information from different network devices that might be deployed in a customer's network environment. Once events have reached the USM Appliance Server, you can use the USM Appliance web UI to view and analyze events, establish policy and correlation rules, investigate and address alarms, and perform other network security operations.

About USM Appliance Network Security Capabilities

USM Appliance is designed primarily to help mid-size organizations effectively defend themselves against today's advanced threats. The USM Appliance platform provides five essential security capabilities in a single console, giving you everything you need to manage both compliance and threats.



Here is a brief description of the essential functions that USM Appliance provides:

- Asset discovery is an essential security capability of USM Appliance. USM Appliance discovers assets in your environment, detects changes in assets, and discovers rogue assets in the network.
- Asset discovery uses passive tools, such as passive operating system fingerprinting and passive service discovery. Asset discovery also utilizes active scanning, which can be scheduled to be performed periodically or can be performed manually.
- Vulnerability assessment, which can be done in unauthenticated or authenticated modes, identifies vulnerabilities or compliance by comparing the installed software on assets with

a database of known vulnerabilities. With authenticated scanning, and using an administrative user account, USM Appliance can scan the assets more effectively. Vulnerability scans can also be scheduled to be performed periodically or performed manually.

- Intrusion detection monitors network traffic for malicious activity, monitors system log messages, and monitors user activity. Intrusion detection for USM Appliance consists of host-based intrusion detection (HIDS) and network-based intrusion detection (NIDS) components.

HIDS can be used to spot problems on host endpoints, and can include file integrity monitoring, rootkit and registry checks. NIDS passive sniffing interfaces can analyze network payload data to monitor for potentially malicious activity.

- Behavioral monitoring provides visibility into traffic patterns and network flows (NetFlow data), which are used to detect anomalies that might indicate security policy violations. Data used for behavioral monitoring and analysis is collected from network devices, flows based on mirrored traffic, and asset availability monitoring.
- SIEM security intelligence combines and correlates collected logs and other data to find malicious patterns in network traffic and within host activity.

USM Appliance draws intelligence from different sources including AlienVault Lab Threat Intelligence. OTX Correlation rules, created by AT&T Alien Labs™, are used to identify patterns associated with malicious activity. OTX threat data provides IP reputation information for OTX pulses and the Indicators of Compromise (IoCs) they include. OTX pulse information also identifies specific threats and how to address them.

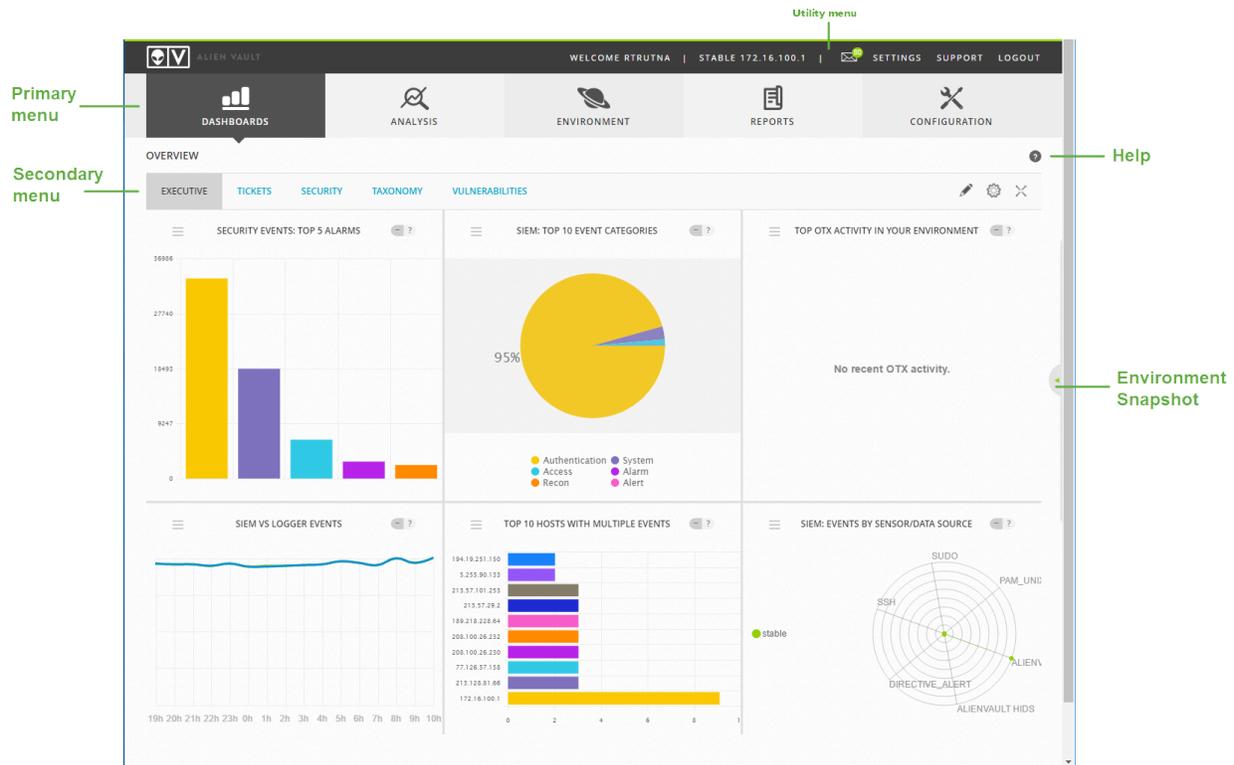
Most USM Appliance security operation features and functionality are accessible from the USM Appliance web user interface (web UI). Additional information on each of the USM Appliance key features is provided in following sections.

The USM Appliance Web User Interface

The USM Appliance web user interface (or web UI) provides access to all the tools and capabilities that USM Appliance makes available for managing security of your organization's network and computers and other devices in the network. From the USM Appliance web UI, you can view all essential information about network devices, applications, user activity, and network traffic in your environment. As you monitor information coming in from devices, you can go about defining and refining policies and correlation directives to fine tune the behavior of your USM Appliance system to alert you of potential security issues and vulnerabilities.

The USM Appliance web UI runs in a standard web browser. Your system administrator can provide the web URL address and credentials to log in and access the features and functions appropriate to your role in your organization's security operation.

When you first log in, the USM Appliance web UI displays the Executive Dashboard.



By default, the web UI displays a collection of high-level graphs and charts summarizing activity in your organization's network. From this main window, you can choose different menu options or click other selectable links and buttons.

Callouts on the screen identify the main navigable elements and selections that are provided consistently through the web UI.

- Utility menu — Displays information on the current user and the USM Appliance IP address or hostname. Also provides options to access the Message Center where in-system errors, warnings, and messages are displayed.
- Settings where you can view (and update) user profile information, and view information on current user activity and sessions. The Settings option includes three menus: My Profile, Current Sessions, and User Activity.

- The My Profile menu shows the personal information (login, name, email) of the user who logged into the system.
- The Current Sessions menu lists who is logged into the system. If you are not the administrator, the administrator must grant you permission in order for you to see this list.
- The User Activity menu shows critical actions that were performed by users. See [Monitor User Activities](#) for more information on using this option to monitor user activities.
- The Support option lets you access the AlienVault Success Center, AlienVault support team tools, and USM Appliance software package downloads. The Support section includes three areas:
 - Help — Provides links to the AlienVault Success Center, to news about the latest releases of USM Appliance, and the Learning Center, where you can find information on how USM Appliance works.
 - Support Tools — This option includes the Remote Support tool that you might use when working with the AlienVault support team. Connecting to Remote Support opens an encrypted connection for AlienVault Support to diagnose any issues with your AlienVault system(s). See Remote Support for more information about using the remote support option to diagnose and resolve USM Appliance issues.
 - Downloads — This option provides links to software packages for AlienVault operation.
- Primary menu — Provides access to the main functions or operations of USM Appliance. These include:
 - Dashboards — Display of all network security charts, tables, and graphs; deployment status and global of the USM Appliance system, network, and devices; and OTX threat and pulse visualizations.
 - Analysis — Display providing search, sorting, filtered selection, and display of Alarms, Security Events (SIEM), Raw Logs, and Tickets.
 - Environment — Provides display and management of Assets & Groups, Vulnerabilities, NetFlow data, Traffic Capture, Availability, and Detection.
 - Reports — Provides display and management of various built-in and custom reports selectable by categories such as alarms, assets, compliance, raw logs, security operations, tickets, and user activities.
 - Configuration — Provides options to view and manage deployed USM Appliance components; Administration options let you manage users, system configuration, and backup and restore settings.

- Secondary menu (or submenu) — For each primary menu selection, there are typically additional secondary or submenu options specific to a particular topic that are displayed when you click the primary selection, for example, **Analysis > Alarms**.
- Help — links to online documentation and topics relevant to the current display and context.
- Environment snapshot — Sidebar display appearing on the right side of the USM Appliance web UI. Unexpanded, the display shows the current alarms and the current Events Per Second (EPS) rate. You can click on the Environment Snapshot tab to expand the display to show more information on open tickets, unresolved alarms, system health, latest event activity, and the number of monitored devices.

The remainder of this guide describes typical best practices in performing common network security operations and provides step-by-step instructions in performing specific tasks. Following sections also describe the USM Appliance web user interface (web UI) from which you can monitor network security and access most USM Appliance security operation features and functionality.

Getting Started with USM Appliance

This section details typical security operations performed after the system installation, initial deployment, and configuration of a USM Appliance has been completed. In addition, this section describes a best practice workflow for using USM Appliance to perform operations during the entire Security Monitoring and Management lifecycle.

This section covers the following subtopics:

USM Appliance Network Security Best Practices	21
What Expectations Should I Have of Security Monitoring?	22
USM Appliance Event Processing Workflow	22
Verifying USM Appliance Operation	24
Establishing Baseline Network Behavior	30

USM Appliance Network Security Best Practices

Providing strong and effective security for an organization's network, IT infrastructure, and environment requires some forethought and planning. If you are now tasked with monitoring, managing, or maintaining network security operations within your organization, after USM Appliance has already been deployed, many of the planning steps and decisions may have already been made, but it is worth reviewing some of the overall best practices that many organizations follow in implementing and then maintaining network security operations in their environments. The general process is the following:

- Determine the scope of your network security operation, the range of networks and sub-networks to be covered, and the network devices or assets (host servers, applications, firewalls, routers, and switches) to be protected.
- Assess risk, determine what is most important to protect, and determine the type of network security you need to provide. Identify specific threats and vulnerabilities you need to address. Also determine specific regulatory compliance and other business standard requirements you need to meet.
- Define and determine security team roles, permissions, tasks, and responsibilities, and implement authentication and authorization to support USM Appliance security operations. Also determine notification and escalation strategy for emails, ticket handling, incident response, and compliance documentation requirements.
- Develop a plan for initial implementation and rollout of network security operations, plus planned updates and enhancements, based on priorities. Take into account the time and resources required for monitoring, incident analysis and response, compliance reporting and record-keeping, plus subsequent updates to address additions or changes in the environment, as well as new threats and vulnerabilities.
- Deploy and run USM Appliance to monitor and analyze the behavior of the environment. Use dashboards, reports, and other features of the USM Appliance web UI to examine events, network traffic, alarms, and notifications. Establish baseline behavior, identify threats and vulnerabilities, and eliminate or reduce false positives and other noise from normal, benign behavior. After establishing a baseline, you can use various tools provided within the USM Appliance web UI to investigate alarms and suspicious events, identify threats and vulnerabilities, and continue monitoring your network for attacks, intrusions, or any other type of malicious and potentially damaging behavior.
- Make continuous security lifecycle improvements and perform regular maintenance: new asset discovery and risk assessments, new vulnerability and threat detection, compliance reporting, backup and archival record-keeping.

- Incident Response — Develop and implement processes and procedures for incident response to provide special event and incident handling. Detect anomalies and suspect behavior; investigate, identify, and isolate threats, intrusions, or attacks; eradicate, remediate, or mitigate threats; conduct post-incident, post-mortem reviews to identify improvements to security processes and practices.

What Expectations Should I Have of Security Monitoring?

Security monitoring is often about monitoring often-overlooked things such as host, device, and application vulnerabilities, because those are typically the same things that attackers will leverage against you later in carrying out attacks or attempting unauthorized access to data or resources. A good network security monitoring system discovers things every day that provide value to security efforts. USM Appliance can help to locate or identify:

- Misconfigured systems.
- Hosts that have fallen off the radar of asset management.
- Systems compromised by opportunistic malware or other attacks by malicious software.
- Inappropriate or unauthorized access of sensitive data or resources from both internal and external parties; for example, detecting websites that should be blocked at the proxy server, but were not.

In most organizations, priorities for network security operations are determined primarily by risk; that is, factors such as the value of assets, the potential damage that particular threats pose, and the likelihood that those threats are realized by actual attack because of specific vulnerabilities or frequency of attacks. Risk to an organization's network and its individual components is also often characterized by its impact based on the following criteria:

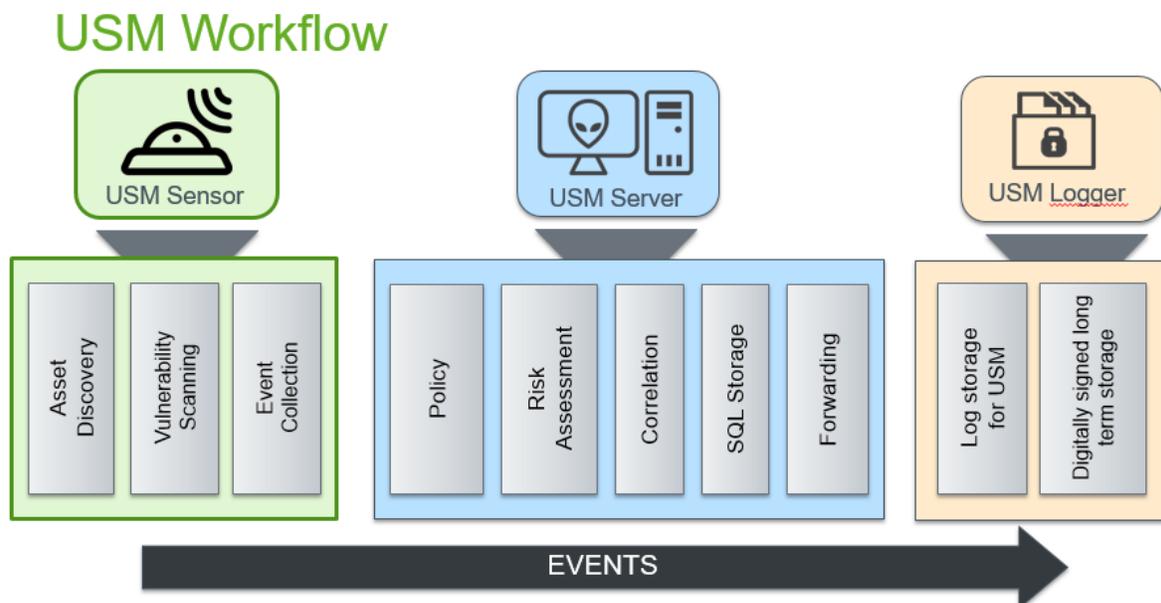
- Confidentiality — guarantees that information can be seen only by authorized users.
- Integrity — guarantees that only authorized users can change sensitive data and information.
- Availability — guarantees uninterrupted access of data, information, and resources by authorized users.

For some organizations, regulatory compliance is also a major factor, due to legal requirements or other factors that create risk to an organization.

USM Appliance Event Processing Workflow

After USM Appliance is installed in your environment, events start flowing through the USM Appliance system, so you can start gaining visibility into what natural or non-threatening activity is taking place, and what worrisome activity, indicating possible attacks, might be taking place. USM Appliance also begins collecting other information about your network and various network devices such as firewalls, routers and switches, servers, and applications. In addition, it is discovering and determining possible vulnerabilities and threats your environment might be susceptible to.

The following illustration details a high level view of events and other information from your network environment as it is collected or generated by USM Appliance Sensors and delivered to the USM Appliance Server for processing.



The USM Appliance Sensor combines asset discovery, vulnerability assessment, threat detection, and behavioral monitoring to provide full situational awareness. The USM Appliance Sensor is the front-line security module of the USM Appliance platform and provides detailed visibility into your environment, vulnerabilities, attack targets and vectors, and services.

The USM Appliance Sensor *normalizes* raw log data and other activity or status information from devices into a standardized USM Appliance event format. These normalized events are then sent to the USM Appliance Server component.

The USM Appliance Server provides a unified management interface through the USM Appliance web UI that combines security automation, and OTX and AT&T Alien Labs™ Threat Intelligence to correlate data, spot anomalies, reduce risk, and improve operational efficiency.

The USM Appliance Server receives events from the USM Appliance Sensor and performs policy evaluation. The policy defines what will happen with events. By default, the events are sent to the correlation engine, from the risk assessment module, and then stored in an internal SQL database. Events can also be forwarded to another USM Appliance Server, if required. This flow is completely configurable using USM Appliance policies.

Correlation can be done logically, where events can be compared to patterns and multiple conditions can be connected by using logical operators such as OR and AND. Correlation can also be calculated using cross-correlation, where events are correlated with vulnerability data. After events are processed and correlated, the USM Appliance Server performs risk analyses and triggers an alarm if the risk of the event is high enough.

The USM Appliance Logger is the secure data archival component of the USM Appliance platform. It stores a copy of all USM Appliance event data that can be used for compliance reporting, or retrieved for later forensics and investigation of past incidents.

Verifying USM Appliance Operation

Once the basic installation and configuration of your USM Appliance system is completed (as described in the *AlienVaultUSM Deployment Guide*), you can use the USM Appliance web UI to verify that it is operating properly.

The following process describes tasks you can perform to verify basic operations, also walking you through information available from the five top-level menu selections:

- When you first launch the USM Appliance web UI, it displays the main dashboards page.



This high-level view of summary information shows the overall state of your network, so you can get an immediate indication of the levels of events and alarms occurring in your environment.

- Confirm that security events are being collected, and populating the USM Appliance database correctly. To see events in the database, navigate to the **Analysis > Security Events (SIEM)** view.

The screenshot displays the AlienVault SIEM interface. At the top, there is a navigation bar with icons for DASHBOARDS, ANALYSIS (selected), ENVIRONMENT, REPORTS, and CONFIGURATION. Below this, the 'SECURITY EVENTS (SIEM)' section is active, showing a search bar and several filter options: DATA SOURCES, ASSET GROUPS, OTX IP REPUTATION, DATA SOURCE GROUPS, NETWORK GROUPS, OTX PULSE, SENSORS, RISK, and ONLY OTX PULSE ACTIVITY. A 'SHOW EVENTS' section on the left allows filtering by time range (Last Day, Last Week, Last Month, Date Range). Below the filters, there are buttons for 'EVENTS', 'GROUPED', and 'TIMELINE'. A 'SHOW TREND GRAPH' toggle is set to 'Off'. The main area displays a table of events with columns: EVENT NAME, DATE GMT-4:00, SENSOR, OTX, SOURCE, DESTINATION, and RISK. The table shows seven rows of events, all with a risk level of 'LOW (0)'. A '675 EPS' badge is visible on the right side of the interface.

On this screen, any normalized log event, or any other event received or generated by any USM Appliance Sensor at the application, system, or network level, appear in the lower portion of the display, unless a USM Appliance policy has filtered it out. In the top portion of the screen, you can further search for and filter out specific events using time ranges and other search criteria. In the tabular list of events, shown in the lower portion of the display, you can click on a specific event row to display additional information for the selected event, in a popup window. You can view and examine full details about an event, in a full browser window, by clicking the  icon in the last column of the event row.

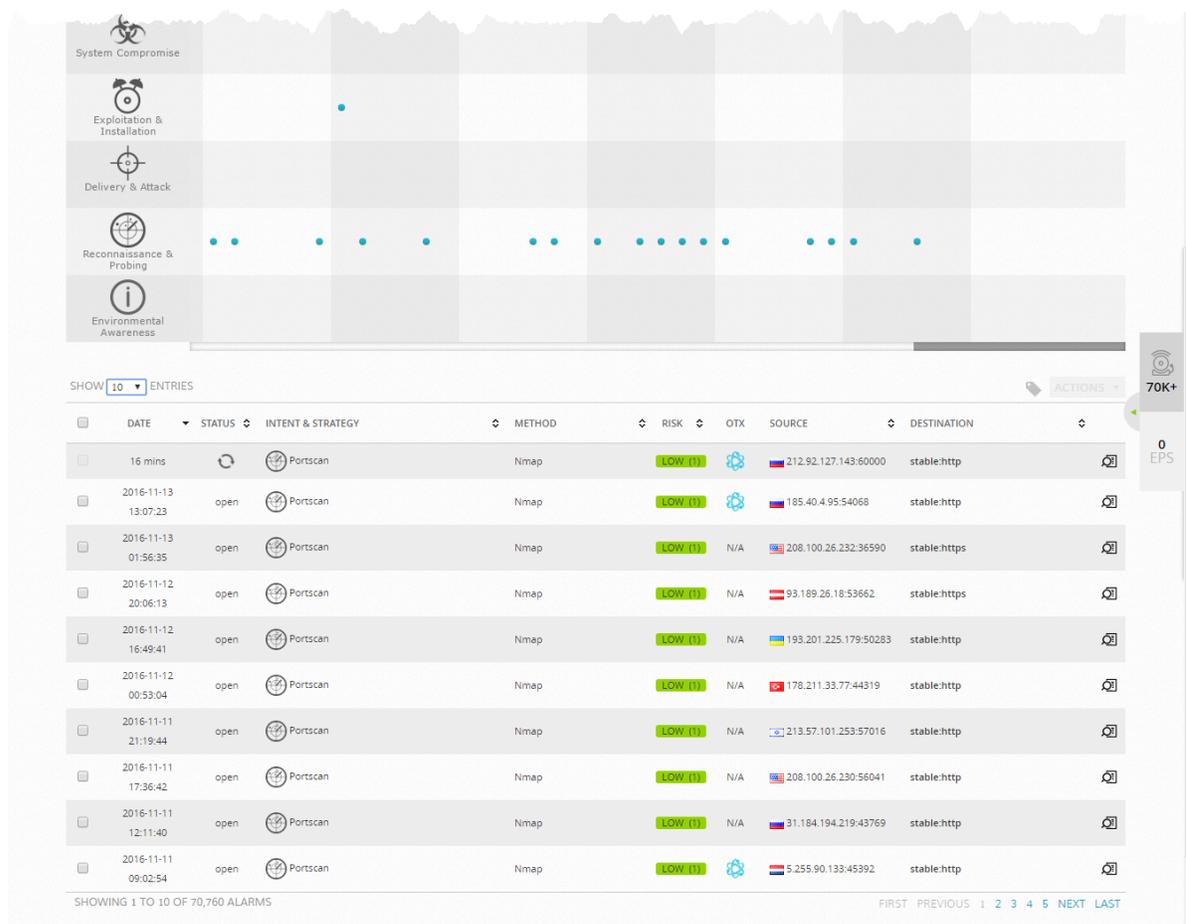
3. Confirm that USM Appliance is creating alarms and the alarms are displaying correctly. The USM Appliance Server uses a formula based on Asset Value, Event Priority, and Event Reliability to calculate an individual event's risk. Any event with a risk of 1 or greater will generate an Alarm. (See [USM Appliance Network Security Concepts and Terminology](#) for a description of how event risk is calculated.)

To see alarms in your system, go to **Analysis > Alarms**.

The screenshot displays the 'ALARMS' section of the Alien Vault interface. At the top, there are navigation tabs: DASHBOARDS, ANALYSIS (selected), ENVIRONMENT, REPORTS, and CONFIGURATION. Below the navigation, the 'ALARMS' section is shown with a 'LIST VIEW' and 'GROUP VIEW' toggle. A search and filter panel is visible, containing various input fields and a 'SEARCH' button. The main area features a graphical representation of alarms over a 31-day period, with blue circles of varying sizes indicating the number of alarms in different categories. The categories are System Compromise, Exploitation & Installation, Delivery & Attack, Reconnaissance & Probing, and Environmental Awareness. The Reconnaissance & Probing category shows the highest number of alarms, with a large blue circle on 16-11-11. The interface also includes a 'SHOW 20 ENTRIES' dropdown and an 'ACTIONS' button.

By default, the middle portion of the screen provides a graphical representation of current alarms being generated in your environment. Blue circles indicate the number of alarms in a category that are appearing at a particular time. A bigger circle indicates a higher number of alarms. Alarms are prioritized by categories that reflect typical methods used by attackers. (See [Alarm Management](#) for more information on alarm categorization.)

The lower part of the window displays a tabular list of alarms.



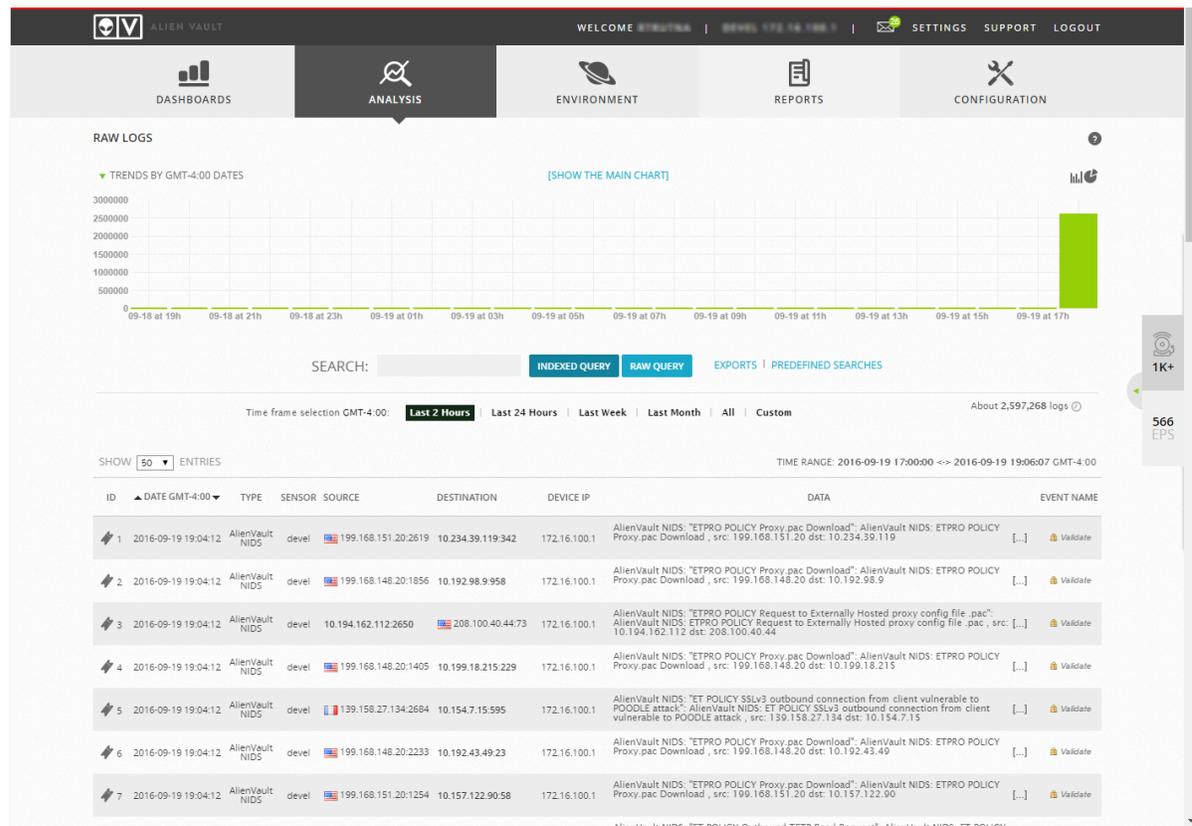
Clicking on an alarm row displays full detail about the alarm, such as the events that triggered the alarm, source and destination IP addresses, and vulnerabilities associated with the alarm.

In the top portion of the screen, you can further search for and filter alarms that are displayed on this page. For example, you can choose to display only alarms originating from a particular sensor, have a certain risk level, or affect only certain groups of assets.

4. Confirm that raw (normalized) log information is being stored in the USM Appliance Logger.

The USM Appliance Logger provides a file-based archive repository that is specially designed to store security log information for long-term archiving and retrieval. Every hour, the archive log files are indexed, compressed and digitally signed to ensure their integrity. You can verify if the USM Appliance Logger component is receiving raw log events from network devices by viewing the data in the Raw Logs screen.

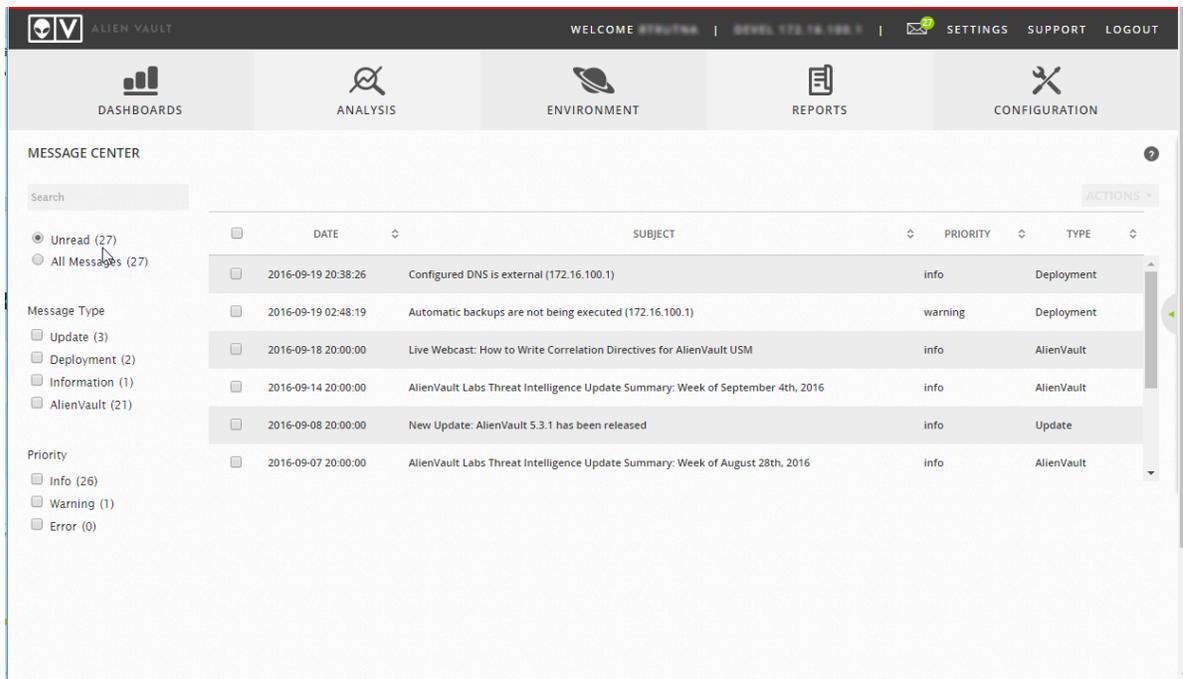
To see the logs, go to **Analysis > Raw Logs**.



The upper part of the window displays a chart, where you can see the log trends in the time frame you have set.

Logs are displayed in the lower part of the window. You can see details about an individual log entry by clicking the corresponding item in the list. You can also use the search box to search for specific log entries, for example, you could search on the name or location of a log file, or the source or destination IP addresses involved in a logged event. You can also select a time range in order to display log entries only for the selected time range.

5. Click the Message (📧) Center icon to observe any system information, error, or warning messages in the Message Center to determine if there are any outstanding issues reported by the USM Appliance Server. The display reports also any issues which occurred with the USM Appliance system components or log collection operations.



The Message Center is where you can receive messages about potential issues with the operation of USM Appliance Server or other components. The Message Center also provides information about available system updates. The USM Appliance web UI displays a list of messages related to any potential issues it detects, in addition to other informational and system update messages.

Establishing Baseline Network Behavior

When you first start using USM Appliance, it is a good idea to let it run for a few days to determine which events and alarms you can consider "noise" and which ones to investigate further. By noise, we mean false positives that obscure true positives, or events that may indicate truly malicious behavior.

Because no system is perfect, you must ensure that you have actionable alarms and useful reports — not hundreds of things to review. What you learn from the baseline collection and the evaluation of those events helps you create policies that tell USM Appliance what is important — or not.

Baselining

To be able to tune the system, you need to create a baseline for what constitutes normal behavior in your network. This is called *baselining*. The alarms and events generated during this initial period represent currently normal behavior, in other words, a snapshot in time. Of course, there may be things you want to filter out right away. But in general, you should resist the temptation and wait until you have had a chance to observe any patterns in your network.

Evaluating Results

After you collect these data points, you need to start making decisions about them, based on the following criteria:

- Which events have value and applicability to my system?
- Which events have to do with network policy and therefore are not potential threats?
- Was the risk properly assessed?
- Which events have value for reporting?
- Who should receive notification when this event occurs?

Answering these questions for the first time is best done in a group setting with the relevant stakeholders. In subsequent iterations of this process, usually only the analysts participate, because the fundamental questions for each event can be applied through taxonomy. Because AlienVault releases new signatures frequently, this decision process should be repeated at regular intervals.

Filtering Out the Noise

Some false positives you may want to identify and filter out right away. One example might be an alarm indicating scanning of hosts in the network. Such activity can be completely legitimate if performed by an internal network mapper. On the other hand, it may be currently benign, but may also be a precursor to a real attack. USM Appliance treats both events equally.

If you examine an alarm and you determine that the event that triggered it was noise, not a real threat, consider taking the following steps:

1. Create a policy that prevents USM Appliance from processing new events from the source. For example, let's say that USM Appliance properly detected vulnerability scanning coming from an internal scanner but such events do not interest you.
2. If not interested in specific alarms, you can do the following:

- Reconfigure the external data source not to send such events.
 - Use a policy to discard such events.
 - Disable the correlation rule.
3. Delete all occurrences of the alarm from SIEM.

Creating New Policies

You may also want to create a policy to reduce the number of false positives. For example, you might create a policy that USM Appliance no longer processes events from the specific host that is the source of false positive events.

Let's say that USM Appliance properly detected vulnerability scanning coming from a vulnerability scanner inside of your system. If you have no interest in such events, because your environment controls the vulnerability scanner, you can create a policy that excludes events coming from it, so that the USM Appliance Server does not process them.

After performing either or both of these tasks, you should delete all occurrences of the alarm from USM Appliance. For information on how to do this, see [Reviewing Alarms as a Group](#).

For more information on tuning correlation rules and policy management, see [Correlation Rules](#) and [Use of Policies in USM Appliance](#).

Tuning Correlation Rules

Tune your correlation rules, if needed, to adjust priority or reliability, or both, to change risk level. If the risk is value lower than 1, USM Appliance does not generate an alarm.

One example in which you might do this would be a correlation rule that detects instant messaging. If your company security policy allows instant messaging, you do not need to receive warnings about such events.

If the alarm was a false positive, in other words, it was triggered by traffic that should not have done so, you must customize the correlation rule that triggered the alarm. After you have customized the rule, label the existing alarm as a false positive, and close it. (For details, see [Reviewing Alarms as a Group](#).)

USM Appliance Security Monitoring and Analysis

This section provides an overview of USM Appliance web UI main menu and submenu options and operations used primarily for display, monitoring, and analysis of network security activities and events.

This section covers the following subtopics:

USM Appliance Dashboards	35
Analyzing Alarms, Events, Logs, and Tickets	41
Managing the USM Appliance Environment	48
USM Appliance Administration and Configuration	59

USM Appliance Dashboards

The first menu selection of the USM Appliance web UI that plays a large part in security monitoring and analysis of a network environment is the Dashboards menu. It provides overall visibility into the activity on your network, and displays various network security metrics.

Dashboards Overview

When you first log in to the USM Appliance web UI, it opens the **Dashboards > Overview** page.





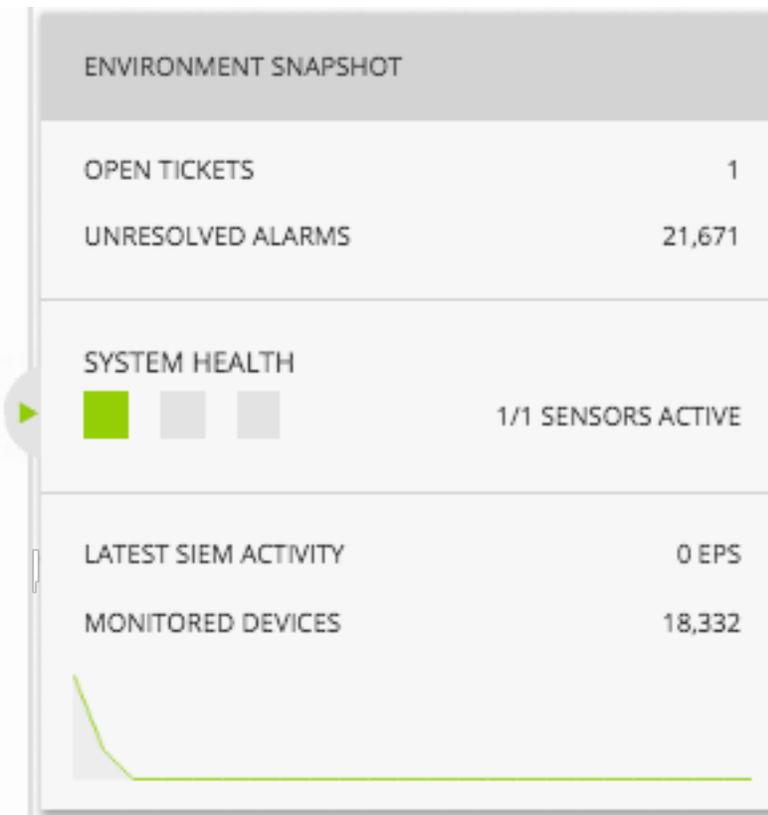
Note: The OTX Activity widget will only contain data when the suspicious IP is reported as an IOC for a pulse. See [OTX Pulses and Indicators of Compromise](#) and [Displaying Alarms and Events Based on OTX Pulse and IP Reputation](#) for details.

The default **Overview > Executive** display shows various “widgets” (charts, tables, and graphs) that summarize various aspects of network security and other status, activities, and events occurring in your network. Additional options from the Overview page provide dashboard displays for Tickets, Security, Taxonomy, and Vulnerabilities.

- **Tickets** — Provides metrics on tickets created within USM Appliance’s own ticketing system.
- **Security** — Provides metrics on different measures of security in the environment, for example, promiscuous host, active hosts, most frequent alarms, and security event reporting trends.
- **Taxonomy** — Provides metrics on events based on different USM Appliance taxonomy event classifications, for example, virus detection, successful and failed logins, malware, and exploit event types.
- **Vulnerabilities** — Provides metrics on vulnerability characteristics such as severity and most affected hosts. Also displays details of available scan reports.

Each widget on the dashboard provides its own representation of information along with a legend or description of data points. For most dashboard displays, you can mouse over or click through portions of the display to view the data on which the dashboard display was rendered. Clicking on the icon provides a more detailed explanation about the information the widget displays. For more information about the dashboard, see [USM Appliance Dashboard Configuration](#).

The Environment Snapshot is displayed on the far right side of the USM Appliance web UI. The default state shows the current alarms and the Events Per Second (EPS). You can expand the Notification Tray to view the Environment Snapshot by clicking on the small arrow on the left side of the summary Environment Snapshot display.



The Environment Snapshot shows open tickets, unresolved alarms, system health, latest event activity, and the number of monitored devices.

In addition to the Overview display, the main Dashboards menu selection also provides several other submenu selections:

- **Deployment Status** — Provides a global view of monitoring in place for assets, networks, and locations. In addition, you can define locations and then add USM Appliance Sensors to monitor and view monitoring in place (such as IDS, vulnerability scan, NetFlow monitoring) for different network devices and servers at a specific location.
- **Open Threat Exchange** — Allows you to visualize threats graphically in a map, as well as list OTX Pulse information. The map visualizes IP addresses that belong to hosts that are performing attacks or have malicious behavior. These IP addresses are provided by Indicators of Compromise which are included as part of OTX pulses.

Deployment Status

To take a closer look at the deployment status of all your networks and assets, go to **Dashboards > Deployment Status**.

DEPLOYMENT STATUS



Al Hajar (3)	Pvt_192 (192.168.0.0/16)	<p>Pvt_010 (10.0.0.0/8) Owner: My Company</p> <p>✓ IDS Enabled</p> <p>✗ Vuln Scan Scheduled</p> <p>✗ Passive Inventory Enabled</p> <p>✗ Active Inventory Enabled</p> <p>✓ Netflow Monitoring Enabled</p> <p>✗ Unclassified Asset List</p>	0 %
Hong Kong (3)	Pvt_172 (172.16.0.0/12)		Network Devices 0/0 Configured
Honolulu (3)	Pvt_010 (10.0.0.0/8)		0 %
Hô Chí Minh City (3)			Servers 0/0 Configured
Lusaka (3)			
Montreal (3)			
Murcia (3)			
México DF (3)			
Olanchito Office (3)			
Oporto (3)			

ADD LOCATION

< PREVIOUS NEXT > < PREVIOUS NEXT >

Here you can see an overview of global visibility, assets visibility, and network visibility at the top of the page. Global visibility lists how many locations are in your environment, and how many of them have sensors deployed. Assets visibility lists the total number of network devices (such as modems, hubs, switches, and routers) and servers in your environment and whether or not they've been configured in USM Appliance. Network visibility displays how many individual networks have IDS enabled, NetFlow monitoring, and how many have scheduled inventory and vulnerability scans.

In the network view, click the **Unclassified Assets** List link at the bottom of the network view pane to define any unclassified assets. Click on **Network Devices** or **Servers** links to see individual details about which assets are configured and when the latest log was created for that asset.

HOSTNAME	IP	LATEST LOG
VirtualUSMStandardServer	10.70.5.136	2017-11-22
Host-10-70-5-22	10.70.5.22	Not received yet
Host-10-70-5-46	10.70.5.46	2017-11-22

Below the header, you can also explore the individual locations and the networks on them. You can click the settings icon (⚙️) to configure network services for the network.

CONFIGURE SERVICES ✕

Select the right configuration for each service

- IDS ON
- Vulnerability Scans ON
- Passive Inventory ON
- Active Inventory ON
- Netflow Monitoring ON

USM Appliance Dashboard Configuration

Within the dashboard view, you can see multiple tabs displaying various visual representations of realtime visual data with its widgets. This is particularly useful for having a quick overview of relevant information and, depending on your needs, it can be further customized to display relevant information to your needs.

The USM Appliance dashboard comes with a set of preconfigured tabs, each with their own set of relevant widgets. These preconfigured tabs cannot be edited, but they can be cloned or hidden. You can create your own tabs with custom widgets or share your custom tabs with other users.

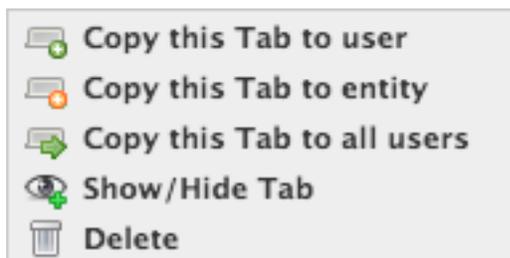
Edit and Customize Tabs

In the default view you see from the **Dashboards > Overview** page, you can click the different tabs to analyze the information from each. You can click and hold the move (☰) icon to drag the widget to a different location on the grid. You can also click the minimize button (— ?) to toggle visibility of the widget or hover over the info icon on the right of the same button for more info on the grid.

Dashboard Permissions

To open the tab edit options on the **Dashboards > Overview** page, click the settings icon (⚙️) to bring up the Dashboard Permissions popup. Here, you can see all of the available tabs, as well as select which tabs are shown on the Overview page, rearrange tabs, and copy tabs to share. Dashboard editing is only available to users with access permissions (see [User Authorization](#) for more information).

You can click the Show Default Tabs text below user names to display the available tabs. Click the edit icon (✎) to display tab options for visibility, sharing, and copying the tabs.



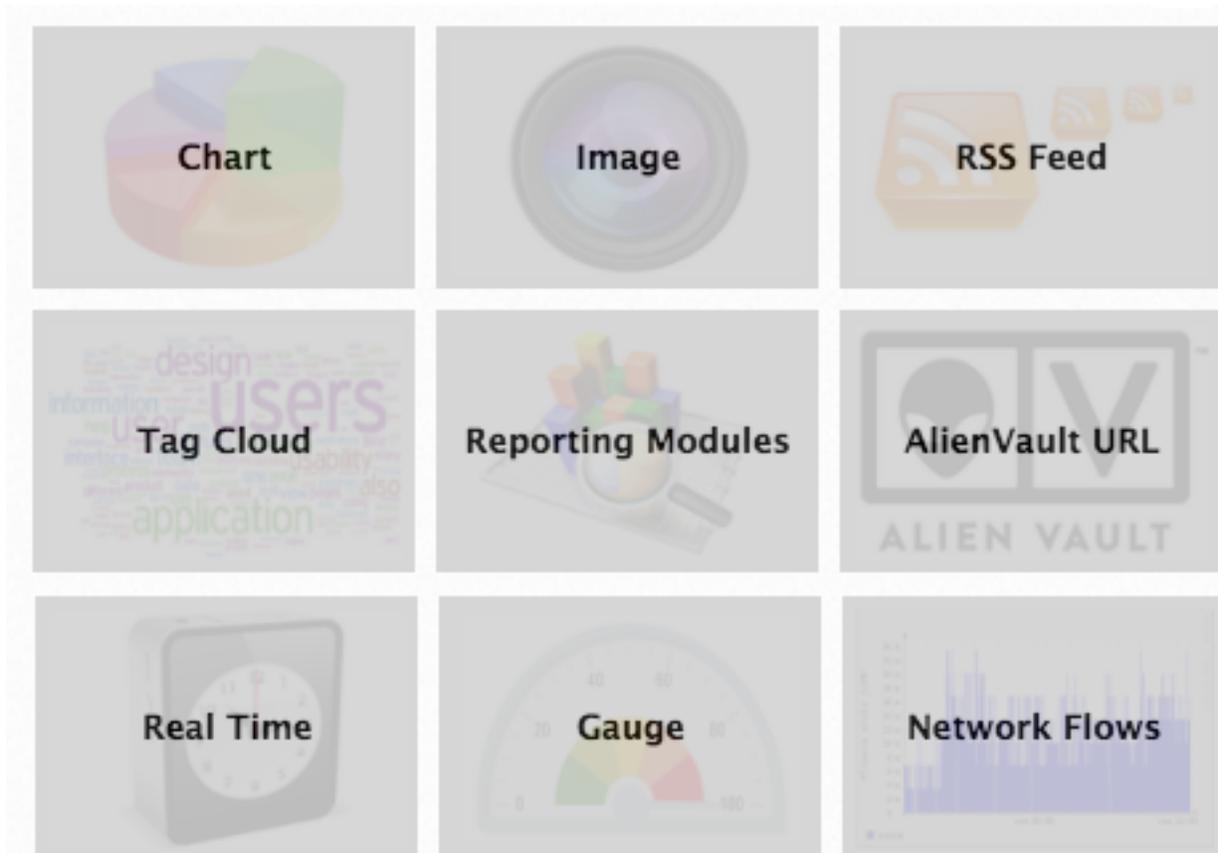
Widget Customization

To edit the tabs, add new widgets, and customize widgets, click the edit icon (✎) on the overview page. From this view you will be able to customize your widget and dashboard settings further.

Click the plus icon (+) at the top left of the tabs header to create a new tab. Here you can name the tab and determine how many columns will be in the widget view for that tab.

Click **Add Widget** to open the Widget Wizard view. Here you can find a number of widget options to create and customize a new widget for your view.

WIDGET WIZARD



Click on any of the widget types to begin customizing the widget. Depending on the type you select, you will be able to further customize the individual options of the widget, you will also be given the option to designate further what kind of information it conveys and, if applicable, which assets it's conveying information from. For the final customization screen, you can give the widget a title and a help description, as well as define the widget's refresh rate, size, and display type.

To edit or delete a widget you've already added, click the edit or trash icon ( ).

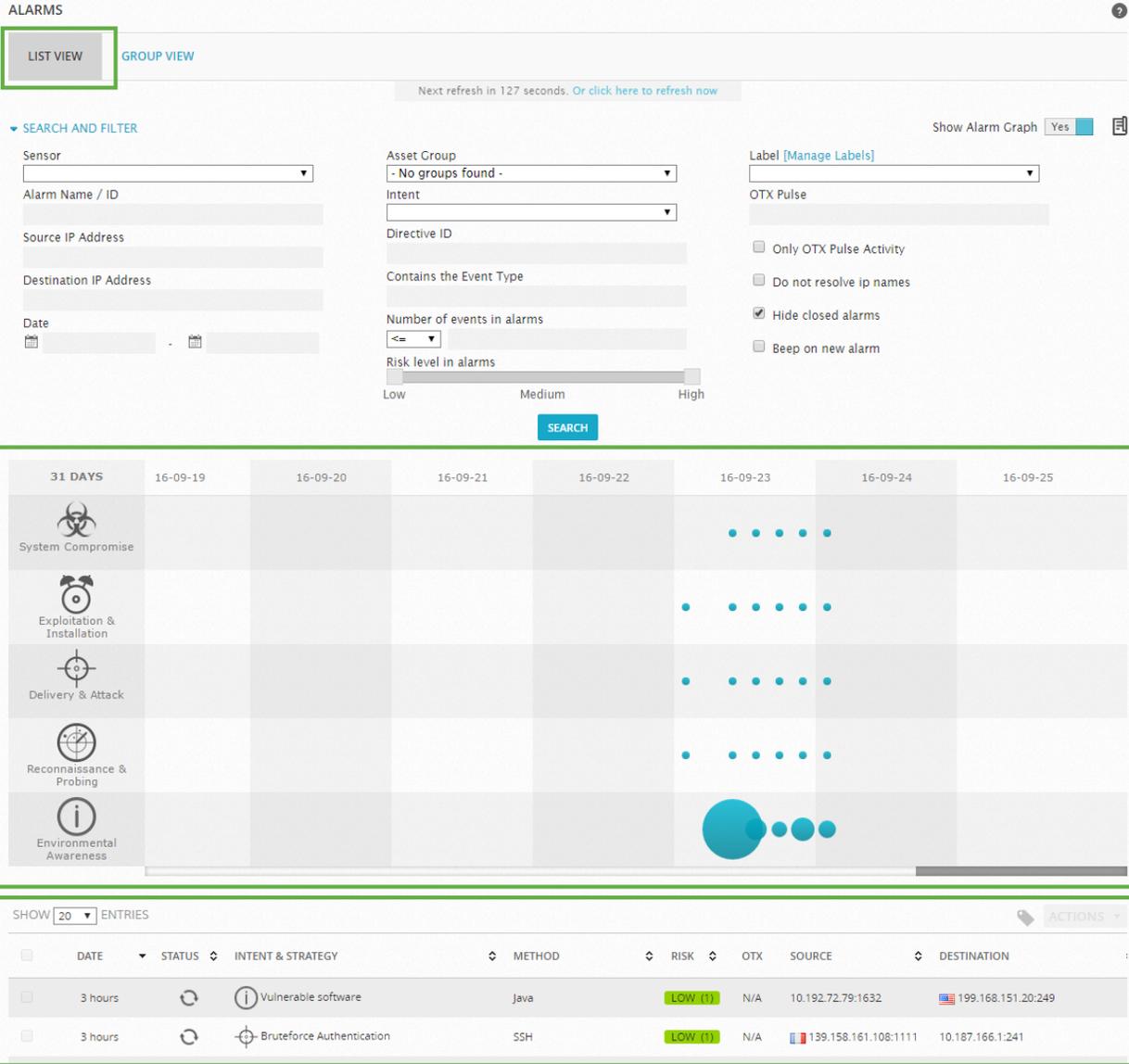
Analyzing Alarms, Events, Logs, and Tickets

You will likely spend the most time reviewing and analyzing the network security of your environment using various options provided in the USM Appliance web UI Analysis menu. The Analysis menu provides the following submenu selections:

- **Alarms** — Shows all the alarms generated in USM Appliance. (Any event with a calculated risk value of 1 or greater generates an alarm.) You can also search for alarms using filters.
- **Security Events (SIEM)** — Displays all events that were processed or generated by the USM Appliance Server. You can also search and filter events that appear in the display as well as view details of specific events.
- **Raw Logs** — Provides access and display all the events that USM Appliance Logger saved to archive log files, for long-term storage and forensic investigation. The USM Appliance Logger digitally signs and timestamps the archived log files, to ensure their integrity and guarantee, for compliance reporting, that the data in log files has not been tampered with.
- **Tickets** — Provides access to USM Appliance ticket management system. Tickets provide workflow tracking of activity related to detected alarms or any other issues that you want to keep track of.

The Alarms Page Display

When you select the **Analysis > Alarms** option, USM Appliance displays the following page.



By default, the display opens in List View, which simply lists alarms in reverse chronological order (the latest issued alarm is displayed first). You can also change the display to Group View, which allows you to group alarms by different keys such as alarm name, source and destination IP address, or alarm type.

The middle portion of the screen includes a table that provides a graphical aggregated representation of alarms that occurred in the last 31 days; each column represents a different day. Blue circles indicate the number of times that an alarm in a category appeared. A bigger circle indicates a higher number of alarms were generated. You can mouse over each of the circles to get the actual number of different types of events that occurred as well as a Top 5 list of possible remedies for each alarm type.

Alarms are sorted into five different categories, which are represented by the graphic icons in the display. These are:

- System compromise ()
- Exploitation and installation ()
- Delivery and attack ()
- Reconnaissance and probing ()
- Environmental awareness ()

The categories are also consistent with the sequence or stages of events that an attacker might follow to successfully infiltrate a network, gain unauthorized access to data, or perform some malicious act. The categories are also consistent with a model of attack detailed by Lockheed Martin called the Cyber Kill Chain.

Below the categorized display of alarm icons, USM Appliance displays a tabular listing of individual alarms, by default, in reverse chronological order. In addition, if you click on any of the blue circles, USM Appliance will display only the alarms corresponding to the selected circle. From the list of alarms, you can click on any individual alarm row to expand the display of information about the alarm. You can then click the **View Details** button, or click the **View Details** () icon, to display more information on the selected alarm, including individual events that actually triggered the alarm.

The top section of the Alarms page display lets you search for and filter alarms that are displayed on the Alarms page. You can qualify alarms by event attributes such as sensor location, asset group, risk level, or OTX pulse.

 **Note:** See [Alarm Management](#) for more information on the operation of Alarms in USM Appliance.

The Security Events (SIEM) Page Display

When you select the **Analysis > Security Events (SIEM)** menu option, USM Appliance displays the following page.

SECURITY EVENTS (SIEM)

SIEM REAL-TIME EXTERNAL DATABASES

Search

SHOW EVENTS

Last Day
 Last Week
 Last Month
 Date Range

DATA SOURCES

ASSET GROUPS

OTX IP REPUTATION

DATA SOURCE GROUPS

NETWORK GROUPS

OTX PULSE

SENSORS EXCLUDE

RISK

ONLY OTX PULSE ACTIVITY

userdata1 like

Device IP

CLEAR FILTERS

ADVANCED SEARCH

EVENTS GROUPED TIMELINE

SHOW TREND GRAPH Off

CHANGE VIEW ACTIONS

DISPLAYING 1 TO 50 OF MILLIONS OF EVENTS. 2,486,895 TOTAL EVENTS IN DATABASE.

EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:1200	10.192.98.57:7	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	208.100.40.44:2431	10.157.4.16:368	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	208.100.40.44:2525	10.196.42.34:503	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:2294	10.234.39.117:251	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.148.20:2294	10.201.68.97:297	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:2674	10.150.2.45:898	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:1232	10.192.78.13:766	LOW (0)

By default, the **Security Events (SIEM)** page displays a SIEM view of events. The USM Appliance web UI also provides two other options for displaying security events:

- **Real-Time** — view that shows events in progress in your network.
- **External Databases** — display security events from an external AlienVault database that is associated with a different AlienVault USM Appliance installation. For more information on configuring a connection to an external AlienVault database, see [How to display Security Events from an External AlienVault Database](#).

From the SIEM option view, you can search and filter for events using time ranges and other event attribute criteria.

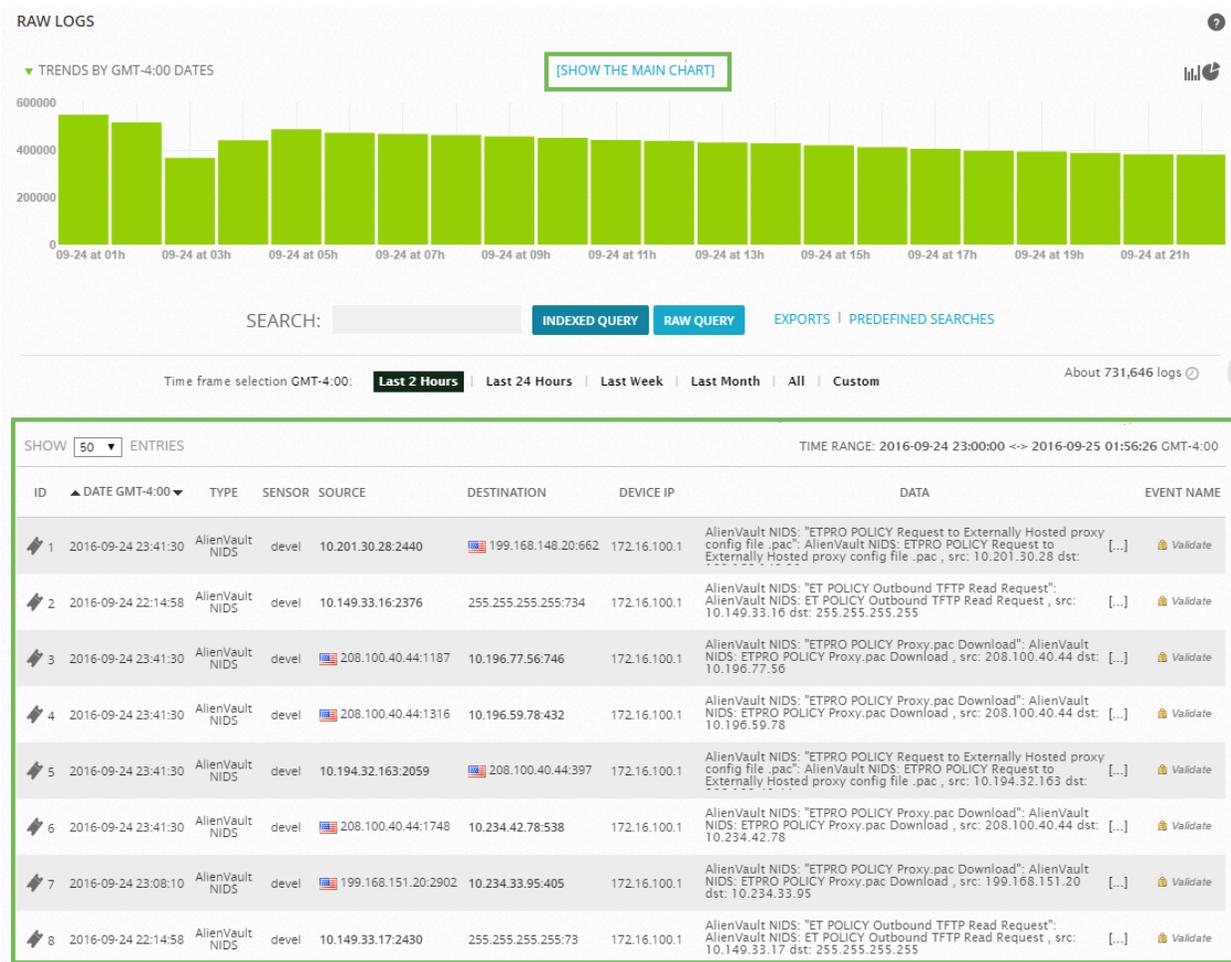
See [Event Management](#) for more information on monitoring analyzing events in USM Appliance.

Below the Search Filter section of the page, USM Appliance provides a display of all events, or filtered events (if you specified search criteria for events). Any normalized log event, or any other event received or generated by any USM Appliance Sensor at the application, system, or network level will appear in the display unless a USM Appliance policy has filtered it out or you have specified search filter criteria.

From the tabular summary listing of events, you can click on a specific event row to view further details about that event in a popup window. You can also click the **More Details** (🔍) icon in an event row to display event detail on a new page, which also lets you choose further actions to take with the current event.

The Raw Logs Page Display

When you select the **Analysis > Raw Logs** option, USM Appliance displays the following page.



This page provides access and display of all the normalized events that USM Appliance Logger saved to its archive log files, for long-term storage and forensic investigation. The USM Appliance Logger digitally signs and timestamps the archived log files, to ensure their integrity and guarantee, for compliance reporting, that the data in log files has not been tampered with. From the Raw Logs page, you can click the Validate (🔒) icon to validate that any particular event has not been altered.



Note: See [Raw Log Management](#) for more information on accessing and using USM Appliance raw logs.

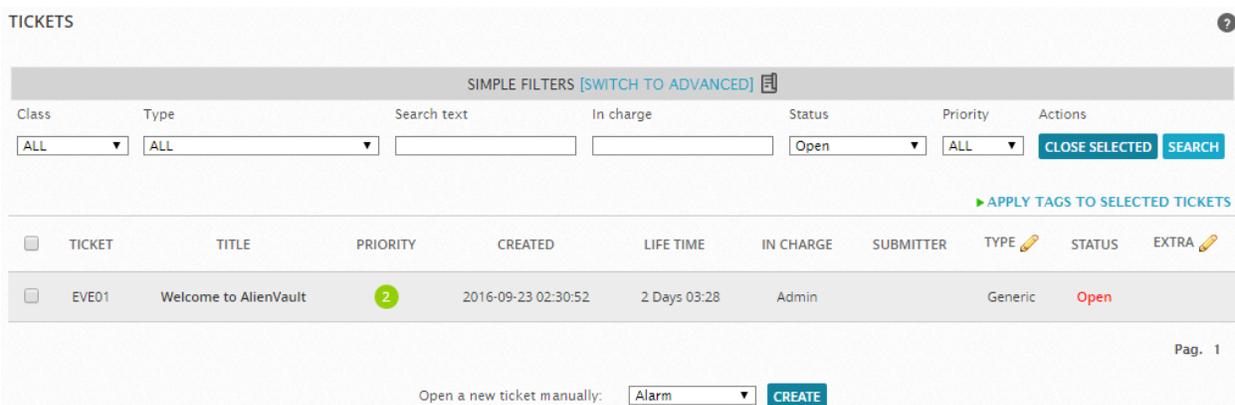
By default, the Raw Logs page displays a raw log event trending graph, which shows the number of events occurring within a specified interval of time. You can click on any of the bars to display only the events that occurred within that time frame.

The USM Appliance web UI provides another option, Show the Main Chart, which provides another view of raw log events. You can also click the View Pie Graphs () icon to alternate the display to a collection of pie charts that show the distribution of events by sensor, event types, sources, and destinations.

Below the trending chart, you can specify the duration of the time frame, such as last 2 hours, last 24 hours, or last week. In addition, you can specify a logical expression search string query to filter the event display. Below the trending chart, and Search areas, the web UI provides a tabular display of events matching a selected time frame, or matching an indexed or raw query.

The Tickets Page Display

When you select the **Analysis > Tickets** option, USM Appliance displays the following page.



TICKETS

SIMPLE FILTERS [SWITCH TO ADVANCED]

Class	Type	Search text	In charge	Status	Priority	Actions
ALL	ALL			Open	ALL	CLOSE SELECTED SEARCH

▶ APPLY TAGS TO SELECTED TICKETS

TICKET	TITLE	PRIORITY	CREATED	LIFE TIME	IN CHARGE	SUBMITTER	TYPE	STATUS	EXTRA
EVE01	Welcome to AlienVault	2	2016-09-23 02:30:52	2 Days 03:28	Admin	Generic	Open		

Pag. 1

Open a new ticket manually: Alarm CREATE

This page provides access to the USM Appliance ticket remediation system. Tickets provide workflow tracking of activity related to detected alarms or any other issues that you want to keep track of. By default, the USM Appliance web UI displays a list of all tickets. In addition, you can click the **Create** button to create a new ticket of a specific type or category.

In the Filters section at the top of the Tickets page, you can choose criteria to filter the ticket results. You can choose additional criteria to filter ticket results by clicking the **Switch to Advanced** option.

From the Ticket summary list, you can click on a specific ticket to open the ticket and display the entire details of the ticket on a new page. From this ticket detail display, you can perform various actions such as editing fields in the ticket, assigning the ticket, adding notes and attachments, and changing the status and priority of a ticket, depending on whatever method or process you want to use to track resolution of issues.

Managing the USM Appliance Environment

In addition to monitoring and analyzing events and alarms, there are other aspects of security you will monitor and update in your network environment. The Environment menu provides access to these other areas of network security through various submenu options, which include the following:

- **Assets & Groups** — This option lets you view and manage assets, networks, asset groups, and network groups.
- **Vulnerabilities** — This option lets you view and vulnerability scanning. The vulnerability scan can run from one or more AlienVault sensors.
- **NetFlow** — This option provides the ability to monitor and work with NetFlow data.
- **Traffic Capture** — This option allows the user to implement and manage remote traffic capture through AlienVault Sensor. There are several capture options such as timeout, packet size, sensor name, and packet source and destination.
- **Availability** — You can use this option to view and configure availability monitoring.
- **Detection** — This option is used to manage intrusion detection for most operating systems. This option also displays log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response.
- **Reports** — Lists all available USM Appliance reports and allows you to perform operations such as Delete, Export, Copy, Edit, Custom Run, and Run Report.

The Assets & Groups Page Display

When you select the **Environment > Assets & Groups** option, USM Appliance displays the following page.

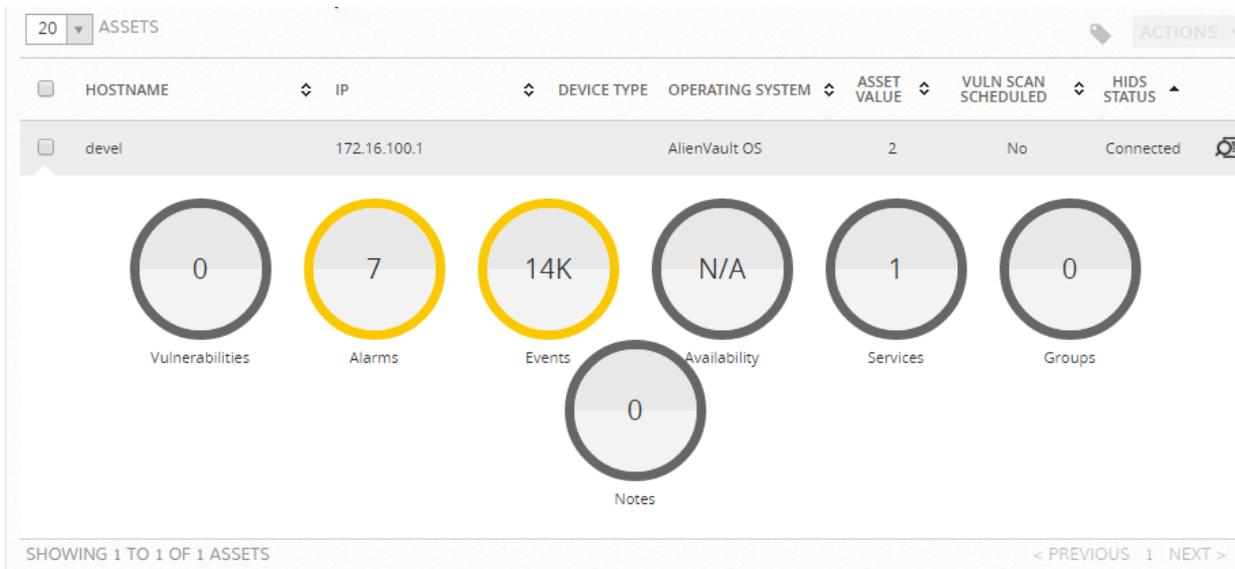
The screenshot displays the 'ASSETS & GROUPS' section of the USM Appliance interface. The 'ASSETS' tab is active. A search panel on the left provides various filters. The main content area shows a summary of 18,335 assets and a table listing 20 individual assets. The table columns are: HOSTNAME, IP, DEVICE TYPE, OPERATING SYSTEM, ASSET VALUE, VULN SCAN SCHEDULED, and HIDS STATUS. Each row includes a checkbox and an 'ACTIONS' button.

HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
stable	172.16.100.1		AlienVault OS	2	No	Connected
Host-192-168-99-95	192.168.99.95			2	No	Not Deployed
Host-192-168-99-92	192.168.99.92			2	No	Not Deployed
Host-192-168-99-9	192.168.99.9			2	No	Not Deployed
Host-192-168-99-89	192.168.99.89			2	No	Not Deployed
Host-192-168-99-85	192.168.99.85			2	No	Not Deployed
Host-192-168-99-84	192.168.99.84			2	No	Not Deployed
Host-192-168-99-81	192.168.99.81			2	No	Not Deployed
Host-192-168-99-80	192.168.99.80			2	No	Not Deployed
Host-192-168-99-8	192.168.99.8			2	No	Not Deployed
Host-192-168-99-78	192.168.99.78			2	No	Not Deployed
Host-192-168-99-77	192.168.99.77			2	No	Not Deployed

The default **Environment > Assets & Groups** display shows a count of assets and also displays a tabular list of all assets in your network environment that were added manually or created using asset discovery (performed by network scans). You can click the **Add Assets** button to add assets, choosing options such as Add Host, Import from CSV, Import from SIEM, and Scan for New Assets. Selecting the checkbox next to a specific asset enables the **Actions** button to select operations such as running asset or vulnerability scans, deploying a HIDS agent, and enabling availability monitoring.

From the default Assets display, the left-side Search panel lets you filter the assets appearing in the asset list by selecting specific asset attributes. USM Appliance maintains an integrated inventory of assets that can store additional information about assets, in addition to information retrieved using passive and active scanning methods and tools.

Clicking on a specific asset in the tabular asset list expands the information displayed for the selected asset. This includes related information such as the number of vulnerabilities, alarms, and events pertaining to the asset.



You can also sort assets in the list by clicking on the table headings that reflect the attribute values maintained for each asset. Clicking the View Details (🔍) icon next to an asset displays all the details recorded or tracked for that asset on a new page.

On the Asset Detail page, besides the name, IP address, and description of the asset, you can also see the location of the asset, plus summary and detail information for related information such as vulnerabilities, alarms, events, and so on.

In addition to the default Assets page view, the USM Appliance web UI also provides the following display options:

- **Asset Groups** — Displays asset information organized by asset groups defined within your network environment. In addition, you can create new groups and add assets from this view.
- **Networks** — Displays asset information organized by networks or subnetworks defined by your organization. In addition, you can add or define new networks or subnetworks to group assets. Assets are organized into networks based on IP addressing.
- **Network Groups** — Displays asset information organized by groups you define within networks or subnetworks. From this view, you can also add new network groups or modify existing ones.
- **Schedule Scan** — Provides options to view existing scheduled scans and schedule new asset discovery scans and WMI scans on Windows hosts.

Note: See [Asset Management](#) for a description of the other Assets page displays and more details on the operations and tasks that you can perform from the Environment > Assets & Groups menu option.

The Vulnerabilities Page Display

When you select the **Environment > Vulnerabilities** option, USM Appliance displays the following page.

VULNERABILITIES

OVERVIEW | SCAN JOBS | THREAT DATABASE

PROFILES | SETTINGS

BY SEVERITY | BY SERVICES - TOP 10

High [6]
 Medium [5]
 Info [150]

TOP 10 HOSTS | TOP 10 NETWORKS

Host-127-0-0-1 [92]

stable [49]

▼ CURRENT VULNERABILITIES

ASSET VULNERABILITY DETAILS

NEW SCAN JOB Service Free text Host/Net **FIND**

HOST - IP	DATE/TIME	PROFILE	SEVERITY	HIGH	MEDIUM	LOW	INFO
All	-	-	0	10	9	0	254
Host-127-0-0-1 (127.0.0.1)	-	-	0	4	4	0	84
	2016-11-02 07:05:32	Default	0	8	8	0	208
	2016-10-06 08:56:31	Default	0	8	8	0	208
stable (172.16.100.1)	2016-11-30 07:09:28	Default	0	2	1	0	46

▼ REPORTS

SCAN REPORTS DETAILS

Date/Time Job Name Host/Net **FIND**

DATE/TIME	JOB NAME	TARGETS	PROFILE	SEVERITY	HIGH	MEDIUM	LOW	INFO
2016-11-30 07:09:28	SCHEDULED - ScheduleTest1	stable	Default	0	2	1	0	46
2016-11-30 03:10:50	SCHEDULED - ScheduleTest2	stable	Default	0	2	1	0	46
2016-11-02 07:07:54	imm	Host-127-0-0-1	Default	0	0	0	0	0
2016-11-02 07:05:32	-	-	Default	0	2	2	0	52
2016-10-06 08:56:31	test	127.0.0.1	Default	0	2	2	0	52

The default Environment > Vulnerabilities display charts the most important vulnerabilities in your environment, by severity and top 10 hosts, or by top 10 services or networks. From this display, you can also view results from past asset vulnerability scans (in HTML or PDF), or

schedule a new scan job. In addition, you can create or edit profiles (describing type of scans that can be performed), and define or edit credentials to be used for scans (by clicking the **Settings** button).

In addition to the Vulnerabilities Overview display, the USM Appliance web UI also provides the following options:

- **Scan Jobs** — Provides capability to view scans in progress, import .NBE vulnerability assessment scan reports, and create or schedule new vulnerability scan jobs.
- **Threat Database** — Provides ability to search for and display current threats.

 **Note:** For more information about threats and vulnerabilities, see [Vulnerability Assessment](#).

The NetFlow Page Display

NetFlow is a protocol designed and published by Cisco Systems that has become the industry standard for recording information about network flows (connections between hosts using TCP/IP). USM Appliance uses NetFlow collection as a service for behavior monitoring. USM Appliance Sensors can collect NetFlow information from traffic received on mirrored ports, or network devices can send net flow information to USM Appliance.

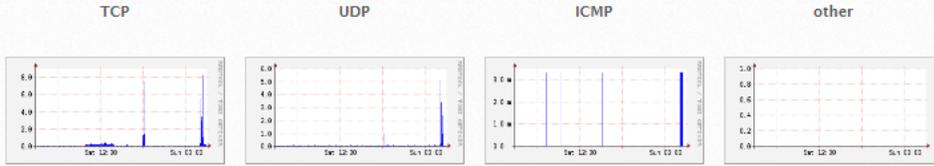
NetFlow collection can assist in identifying insecure services, protocols and ports that are not allowed. It also can assist in identifying traffic sources and destinations to help ensure that inbound internet traffic is limited to IP addresses within the DMZ.

When you select the **Environment > NetFlow** option, USM Appliance displays the following page.

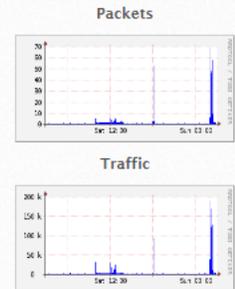
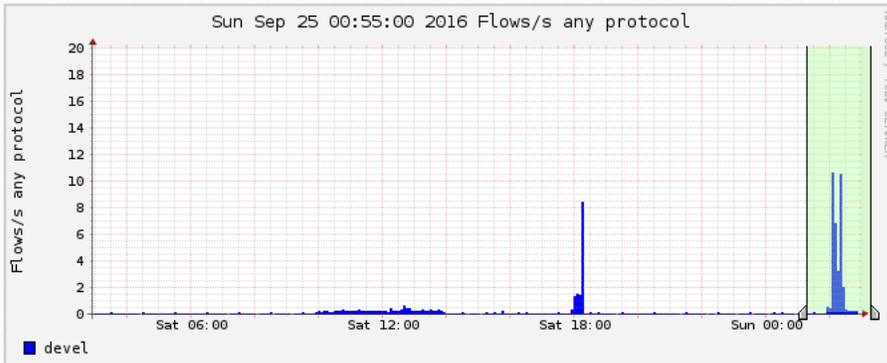
NETFLOW

DETAILS OVERVIEW GRAPH

Profile: live



Profile info:
 Type: live
 Max: unlimited
 Exp: never
 Start: Sep 23 2016 - 02:35 EDT
 End: Sep 25 2016 - 02:55 EDT
 tstart 2016-09-25-00-55
 tend 2016-09-25-02-55



Select Time Window

Display: 1 day

Lin Scale Stacked Graph
 Log Scale Line Graph

STATISTICS TIMESLOT SEP 25 2016 - 00:55 - SEP 25 2016 - 02:55

CHANNEL	FLOWS					PACKETS					TRAFFIC				
	all	tcp	udp	icmp	other	all	tcp	udp	icmp	other	all	tcp	udp	icmp	other
<input checked="" type="checkbox"/> devel	1.5 /s	1.0 /s	0.5 /s	0.0 /s	0 /s	10.4 /s	9.9 /s	0.6 /s	0.0 /s	0 /s	29.9 kb/s	29.5 kb/s	410.2 b/s	1.0 b/s	0 b/s
TOTAL	1.5 /s	1.0 /s	0.5 /s	0.0 /s	0 /s	10.4 /s	9.9 /s	0.6 /s	0.0 /s	0 /s	29.9 kb/s	29.5 kb/s	410.2 b/s	1.0 b/s	0 b/s

ALL NONE Display: Sum Rate

Netflow Processing

[LIST LAST 500 SESSIONS](#) | [TOP 10 SRC IPS](#) | [TOP 10 DST IPS](#) | [TOP 10 SRC PORT](#) | [TOP 10 DST PORT](#) | [TOP 10 PROTC](#)

SOURCE FILTER OPTIONS

devel

and <none>

List Flows Stat TopN

Limit to: 20 Flows

Aggregate

Sort: start time of flows

Output: extended / IPv6 long

CLEAR FORM PROCESS

The default Environment > NetFlow display provides various charts, graphs, and tables to detail statistics about network flows in your environment. You can select the time frame for the NetFlow information displayed by moving sliders in the graph, or by selecting a predefined time range. You can also select NetFlow processing options and specify an additional NetFlow filter such as:

```
ip host x.x.x.x
```

NetFlow data provide information about the session traffic in your environment. Flow information typically captures session details such as the network interface, source and destination IP addresses, source and destination ports, type of service, and so on. NetFlow capture can also include information such as number of packets and bytes in flow, and packet and bit transfer speeds.



Note: For more information on using NetFlow to view network flows in your environment, see [NetFlow Monitoring](#).

In addition to the default Details view, the USM Appliance web UI also provides the following options:

- **Overview** — Displays a collection of chart plotting individual NetFlow attributes such as flows and packets per second. You can click on a specific chart to display more NetFlow detail.
- **Graph** — Displays charts of flow and bit rates based on selection of NetFlow, packets, or traffic options.

The Traffic Capture Page Display

When you select the **Environment > Traffic Capture** option, USM Appliance displays the following page.

TRAFFIC CAPTURE

SENSORS STATUS

SENSOR NAME	SENSOR IP	TOTAL CAPTURES	STATUS
devel	172.16.100.1	0	Idle

▶ HIDE CAPTURE OPTIONS

CAPTURE OPTIONS

TIMEOUT: 10 seconds | CAP SIZE: 4000 packets | RAW FILTER:

SETTINGS

SENSOR: 172.16.100.1 (devel / eth0)

SOURCE:

DESTINATION:

All Assets
 Assets
 Asset Groups
 Networks
 Network Groups

LAUNCH CAPTURE

The Environment > Traffic Capture displays provides options to set up traffic capture of packets and display the results. In setting up the traffic capture, you can specify the duration of the capture (timeout), number of packets to capture, and a selection of asset source and destination addresses of the traffic.

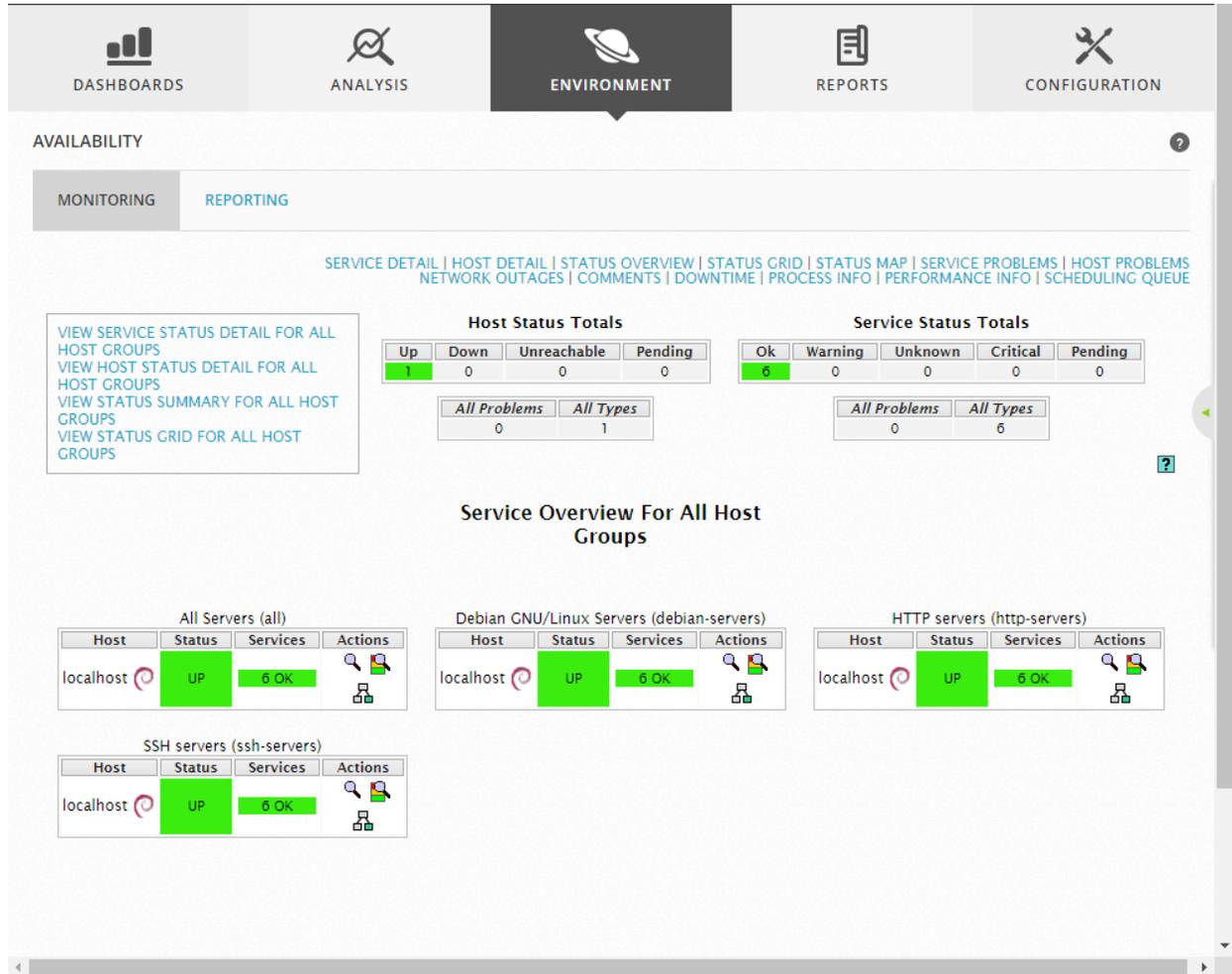
You can click **Launch Capture** to begin the capture. After USM Appliance completes the traffic capture, it displays a traffic capture results page. From the traffic capture results page, you can examine the packets and choose options such as Download or View Payload to view, for example, in an external packet capture tool such as Wireshark.



Note: For more information on performing operations using the Traffic Capture option, see [Capture and Examine Packets](#).

The Availability Page Display

When you select the **Environment > Availability** option, USM Appliance displays the following page.



Within the Monitoring page view, you can select various options to see status details on the localhost. You also can select options to view details such as service and host problems, network outages, downtime, and performance. The default Assets & Groups > Assets page displays status and other operational information on different servers, applications, and services running in your network environment.

In addition to the Monitoring page view, USM Appliance also provides a Reporting page view option that lets you select and generate reports for many of the same details as shown in the Monitoring view. See [About USM Appliance Reports](#).

The Detection Page Display

When you select the **Environment > Detection** option, USM Appliance displays the following page.



The default Environment > Detection page display provides options to manage intrusion detection for most operating systems. You can also display status and other results for intrusion detection, such as event trends, log analysis, integrity checks, Windows registry monitoring, and root kit detection.

From the default HIDS page view (Overview), you can also choose options to display HIDS status and intrusion detection configuration details for the following:

- **Agents** : Review and update settings for HIDS Agent Control, Syschecks, and agents.conf, or add new agents.
- **Agentless** : Review and update settings for agentless intrusion detection on a host.
- **Edit Rules**: Review and update XML rule files and individual rules for HIDS.
- **Config**: Review and update which XML Rules files are either enabled or disabled, set

Syschecks options, and review and edit the Configuration XML file used for HIDS.

- **HIDS Control:** Review and set HIDS Control actions, restart HIDS services, and view HIDS and Alerts logs.

Generating Reports

While the Dashboards menu provides visibility and display of various network security metrics for your network environment, USM Appliance also provides over 200 different reports that you can schedule or generate on demand, which provide detail on various aspects of USM Appliance network security.

The Reports Page Display

When you select the **Reports > All Reports** menu option, USM Appliance displays the following page.

The screenshot displays the 'REPORTS' page in the USM Appliance interface. At the top, there is a navigation bar with icons for DASHBOARDS, ANALYSIS, ENVIRONMENT, REPORTS (selected), and CONFIGURATION. Below this, the 'REPORTS' section has sub-tabs for ALL REPORTS, MODULES, LAYOUTS, and SCHEDULER. A search bar is present, and a dropdown menu shows '20' reports. A sidebar on the left lists categories with checkboxes: Alarms, Assets, Compliance, Raw Logs, Security Events, Security Operations, Tickets, User Activity, and Custom Reports. The main area contains a table of reports with the following columns: REPORT, CATEGORY, SETTINGS, SCHEDULED, and ACTIONS.

REPORT	CATEGORY	SETTINGS	SCHEDULED	ACTIONS
Activity from OTX Pulses	Security Events	Assets: All Assets Date Range: Last 30 days Layout: Default	No	[Icons]
Activity with OTX IP Reputation	Security Events	Assets: All Assets Date From: 2016-01-05 Date To: 2016-02-03 Layout: Default	No	[Icons]
Alarm Report	Alarms	Assets: All Assets Date Range: Last 30 days Layout: Default	No	[Icons]
Asset Report	Assets	Assets: All Assets Date Range: Last 30 days Layout: Default	No	[Icons]
Availability Report	Assets	Assets: All Assets Date Range: Last 30 days Layout: Default	No	[Icons]
Business and Compliance	Compliance	Assets: All Assets Date Range: Last 30 days Layout: Default	No	[Icons]
Database Activity	Security Events	Assets: All Assets Date Range: Last 30 days Layout: Default	No	[Icons]
Events by Data Source	Security Events	Assets: All Assets Date Range: Last 30 days Layout: Default	No	[Icons]

This page displays the entire collection of reports available in USM Appliance, showing the name of each report, its categories, report settings, and whether the report is scheduled to be generated. From this page, you can also select checkboxes in the left-side Search panel to restrict the display to show only those reports belonging to selected categories.

Each of these report categories is also available as a report submenu option, for example, you can select **Reports > Alarms** to display a list that only contains reports pertaining to Alarms.

The last column in the list of reports describes available actions for a selected report. These include Delete, Export, Copy, Edit, Custom Run, and Run Report. You can generate or run a report, on demand, or create a scheduler task to periodically run a report. After you run reports, you can save them as PDFs for printing, or distribution by email.

Clicking the **Actions** button provides options to create or import a new report.

In addition to the default display pages from which you can access and run reports, USM Appliance provides alternative page views for the following:

- **Modules** — Provides selection from over 2600 report components to be included in reports. You can define queries to retrieve data used to generate graphs and tables included in reports.
- **Layouts** — Provides options to define the graphical aspects of reports by defining the header and footer, color scheme, and icons that report documents will use.
- **Scheduler** — Provides options to specify the periodic generation of reports, also designating who can view a report and who reports are sent to.

For more information on creating reports, setting options, and running reports, see [About USM Appliance Reports](#).

USM Appliance Administration and Configuration

During the course of using USM Appliance to manage and maintain network security in your environment, numerous changes will likely take place that will require you to make updates. Networks will change, assets will be added, upgraded, or removed; security objectives may change, and new threats and vulnerabilities will require you to adopt new tools and methods of detecting them. The Configuration menu provides the access to perform many of these tasks through various submenu options, which include the following:

- **Administration** — Provides options to manage users, system configuration, and backup and restore settings.
- **Deployment** — Provides options to configure and manage USM Appliance components.

- **Threat Intelligence** — Provides options to configure USM Appliance policies, actions, ports, directives, compliance mapping, correlation rules, data sources, and security classification (taxonomy). You can also review and edit the knowledge base, which contains information and recommended actions for different types of security incidents.
- **Open Threat Exchange (OTX)** — Provides options to configure OTX settings and view individual OTX pulses and indicators of compromise (IoC) in a separate OTX browser window.

The Administration Page Display

When you select the **Configuration > Administration** option, USM Appliance displays the following page.

ADMINISTRATION

USERS MAIN BACKUPS

USER INFORMATION | ACTIVITY | TEMPLATES | STRUCTURE

SHOW 20 ENTRIES NEW MODIFY DELETE SELECTED DUPLICATE SELECTED MULTILEVEL TREE

LOGIN	NAME	EMAIL	VISIBILITY	STATUS	LANGUAGE	CREATION
avuser1 	avuser1		My Company	✓	English	-
avuser2 	avuser2		My Company	✓	English	-

The default **Configuration > Administration** display (labeled User Information) shows login and user information about current users. Users accessing this page can double-click on the row in the table containing their login name to view and update their own user profile information, including the ability to change their login username, email address, and password.

From the **Users** page, users can also choose the following display options:

- **Activity** — View and choose activities or actions that are logged.
- **Templates** — View and update user access to different sections of the USM Appliance web UI.
- **Structure** — View and make updates to the Asset and Inventory structures maintained by USM Appliance.

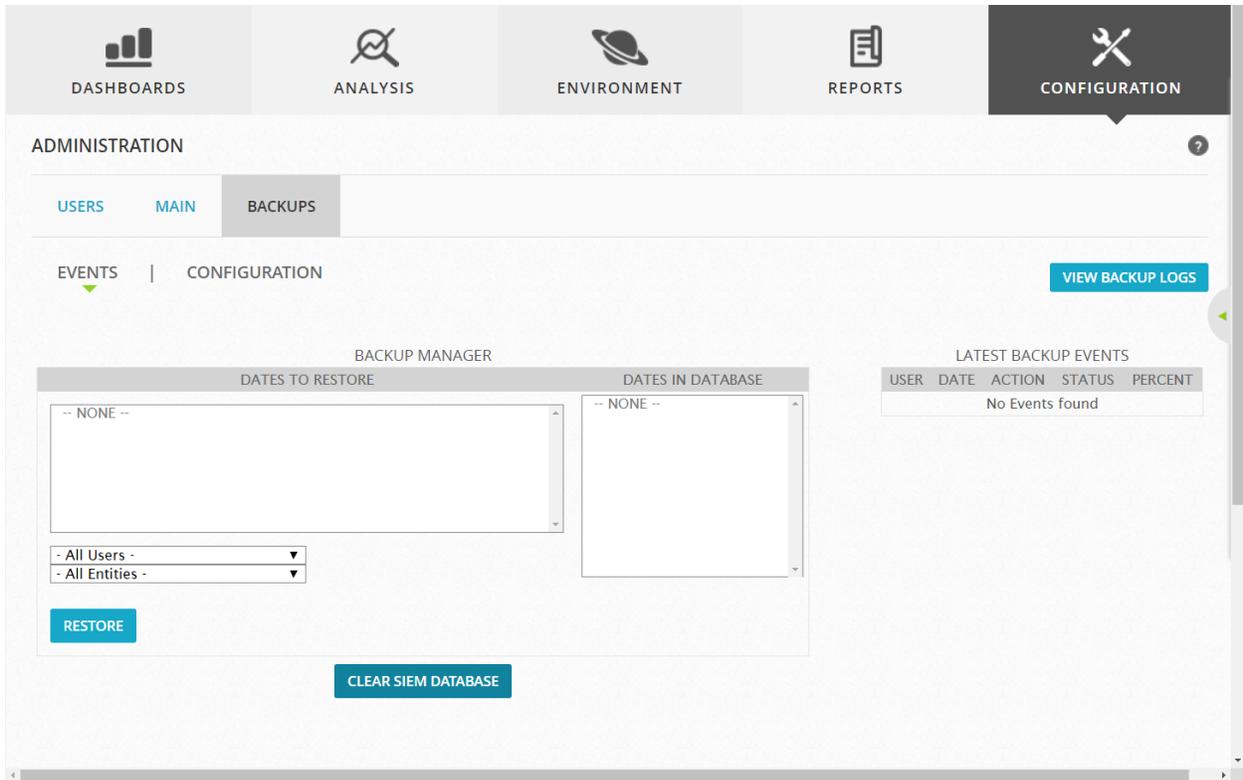
In addition to the main **Users** page view, the web UI provides selections to show two other page views:

- **Main** — Provides options to view and update configuration settings for a number of USM Appliance features and functions that include Backup, IDM (identity management), Tickets, Login Methods, Metrics, USM Appliance Framework, Password Policy, User Activity, and Vulnerability Scanner.

The screenshot displays the 'ADMINISTRATION' section of the web UI. At the top, there are three tabs: 'USERS', 'MAIN' (which is selected and highlighted in grey), and 'BACKUPS'. Below the tabs is a list of configuration categories, each with a green downward arrow on the right side. To the right of the list, there is a search bar labeled 'Find Word' with a 'SEARCH' button. Below the search bar are two prominent blue buttons: 'ENABLE DESKTOP NOTIFICATIONS' and 'UPDATE CONFIGURATION'. A help icon (?) is visible in the top right corner of the administration header.

Category	Action
BACKUP	▼
IDM	▼
TICKETS	▼
LOGIN METHODS/OPTIONS	▼
METRICS	▼
USM FRAMEWORK	▼
PASSWORD POLICY	▼
USER ACTIVITY	▼
VULNERABILITY SCANNER	▼
NETFLOW	▼
AUTOMATIC UPDATES	▼

- **Backups** — Provides options to view backup logs and also view and update Backup Manager settings. Daily backups include all system configuration information including system profile, network configuration, asset inventory data, policy rules, plugins, and correlation directives.

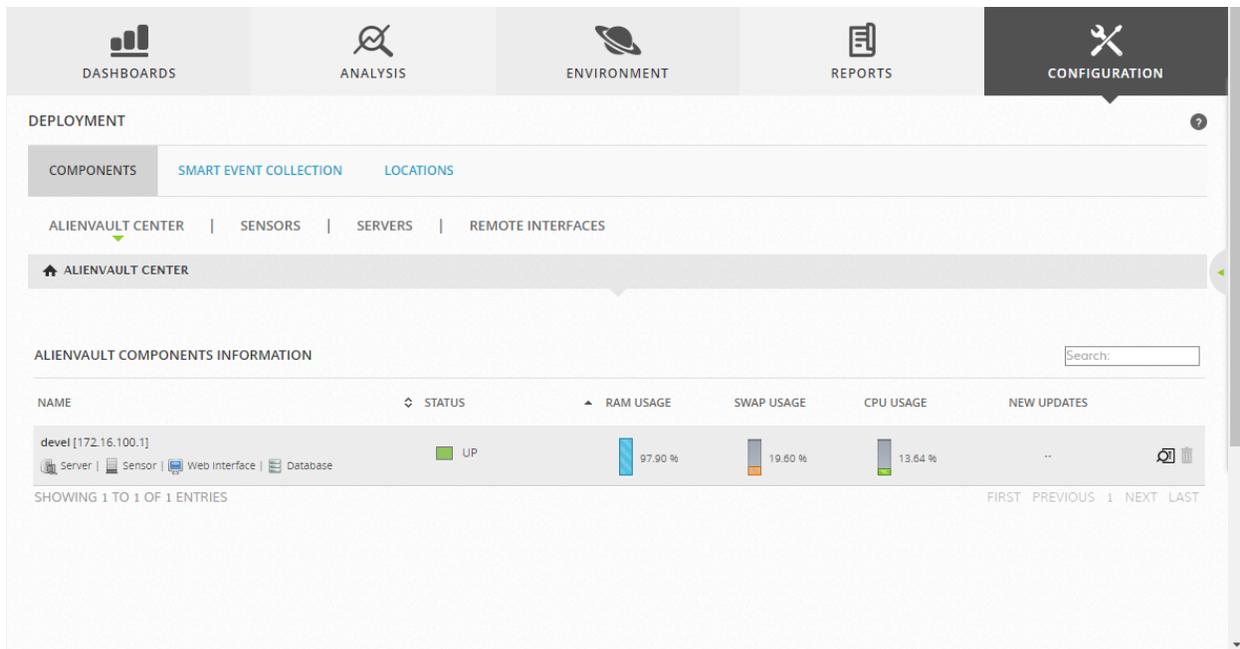


From the **Backups** page, users can also choose the following display options:

- **Events** (the default) — View event backup logs available to restore. See Backing Up and Restoring Events.
- **Configuration** — View configuration backups available to restore. See Backing Up and Restoring System Configuration.

The Deployment Page Display

When you select the **Configuration > Deployment** option, USM Appliance displays the following page.



The default **Configuration > Deployment** display provides status and resource information for different USM Appliance instance components: AlienVault Sensors, USM Appliance Servers, and USM Appliance Loggers. Clicking on a selected component displays additional configuration detail, so that you can view and change configuration settings for existing components. The different page views for these categories also allow you to add and configure new components.

From the Components page, users can also choose the following display options:

- **AlienVault Center** (the default) — View status and resource usage statistics for USM Appliance components.
- **Sensors** — View information on deployed sensors.
- **Servers** — View information and status of deployed USM Appliance Server hosts.
- **Remote Interfaces** — Specify remote interface connections to additional, external USM Appliance devices. Once configured, users can quickly connect to these remote devices to display information about those devices. Selecting a remote interface launches a new window to log in and connect to the web interface of the associated USM Appliance device.

In addition to the Components page view, the USM Appliance web UI also provides the following **Deployment** page selections:

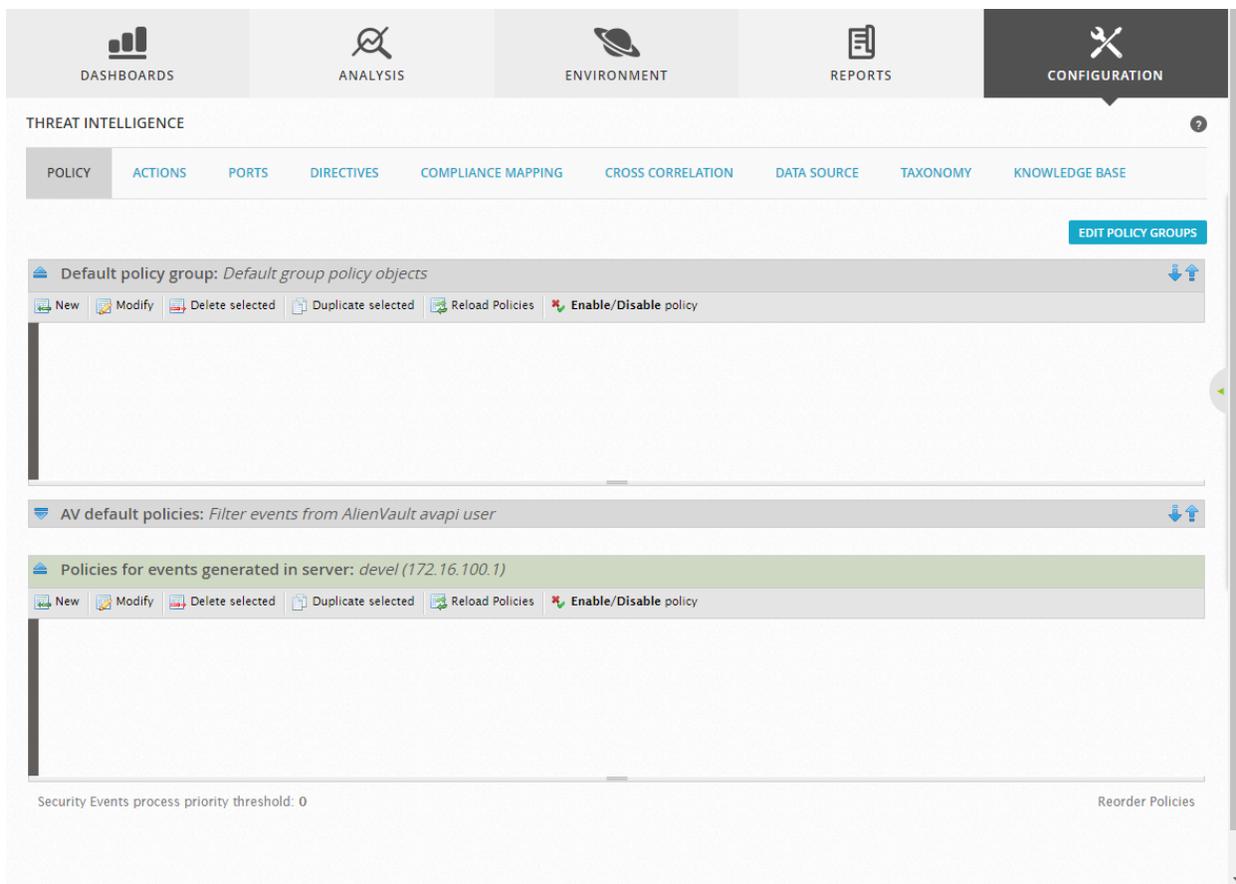
- **Smart Event Collection** — Allows you to point to an existing log file, parse the log, and automatically generate parsing rules for events found in the log. You can then fine tune the configuration to generate a ready-to-deploy USM Appliance Sensor plugin.
- **Location** — Provides options to view and modify USM Appliance network locations. You can also define new locations and add sensors to collect events for that location.

Threat Intelligence Page Display

AlienVault Threat Intelligence improves the effectiveness of your security monitoring efforts by helping you understand why alarms are generated. This allows you to evaluate more easily whether the events associated with an alarm are of real concern. Or, if the events triggering an alarm reflect normal behavior, you can modify policies to eliminate false positives.

 **Note:** You might also consider unsubscribing to OTXpulses whose Indicators of Compromise are creating too much noise and generating false positive alarms in USM Appliance.

When you select **Configuration > Threat Intelligence**, USM Appliance displays the following page.



The **Configuration > Threat Intelligence** display provides options for configuring USM Appliance policies, actions, ports, directives, compliance mapping, cross-correlation, data sources, and security classification (taxonomy). You can also review and edit knowledge base articles, which contain information describing possible attacks and recommended actions for combatting different types of security threats.

- From the Policy page view, you can configure USM Appliance policies. Policies can be configured separately for events (from network devices) and correlation directive events (generated by USM Appliance Server). You can also configure policy groups, which allow you to group policies for administrative purposes.

By default, three policy groups exist that are displayed on this page; the Default policy group, the group for default policies, and the group of policies for events generated in server. You can create your own policy groups by clicking **Edit Policy Groups** and then providing a name for the group.

For more information on creating and modifying policies, see [Create a New Policy](#).

- From the **Actions** page view, you can configure actions to take in response to a specified condition, which may be an alarm or the logical expression of a condition. Actions include sending an email message, creating a USM Appliance ticket, or executing an external program or script. In defining an action, USM Appliance provides a list of keywords that you can specify that will be substituted within any field of the action definition.

For more information on creating actions, see [Create an Action](#).

- From the **Ports** page view, you can view current assignments of ports used by USM Appliance and also add new ports you want to use for other services, mirrored ports, network taps, scans, and so on. In addition, you can view, modify, or create new port groups.

For more information on assigning ports, see [Create Policy Conditions](#).

- From the **Directives** page view, you can view, modify, or clone existing correlation directives. You can also create and test new directives. All pre-defined directives are listed under the AlienVault directive, separated into a number of different categories, based on the specific method of attack or intrusion that the directives address. Any custom directives are listed under the User Contributed section.

AlienVault comes preconfigured with almost 3,000 directives. You cannot delete or directly edit the predefined directives provided by AlienVault; however, you can clone, enable, or disable them. Correlation directives have a unique ID, meaningful name, and a description of the intent, strategy, or method of attack the directive is meant to detect. The directive also assigns a priority according to the likely impact of the detected attack, which USM Appliance uses in the risk calculation of a directive event.

For more information on creating and using correlation directives, see [Correlation Directives](#).

- From the Compliance Mapping page view, you can view and update coverage of security controls to meet ISO 27001, PCI DSS 2.0, and PCI DSS 3.0 compliance regulations, if specified. For each regulation, you can review each requirement, determine if security controls are implemented, and view what data sources and directives are used, or are available, to check compliance for a specific compliance requirement. In addition, you can click **Run Scripts** to run scripts defined for a specific compliance regulation.

For more information on configuring USM Appliance to meet specific regulatory compliance standards, see [Using USM Appliance for PCI Compliance](#).

- From the **Cross Correlation** page view, you can view and modify existing cross-correlation rules and the associated data sources used to collect data to check the associated rule. You can also create new cross-correlation rules or delete rules. Clicking on a specific cross-

correlation rule displays the detail of the rule definition, where you can change the data source and reference for the rule, the event type, and the reference SID name.

Cross-correlation correlates two different types of events, detected by two different data sources. It generates a new event when two related events, detected by different data sources, are detected and the same asset is involved. For more information on creating and using cross-correlation rules, see [Cross-Correlation](#).

- From the **Data Source** page view, you can view and edit details of data sources, which refer to all applications or devices (most commonly, plugins) that generates information that USM Appliance can collect, analyze, and translate into an event within the USM Appliance taxonomy. Each data source also describes every possible event that might occur, to enable USM Appliance risk assessment and correlation to match policies. USM Appliance also lets you organize data sources into Data Source Groups, which makes it easier to incorporate multiple data sources into one policy.

For more information on creating and using data sources, see "Developing New Plugs" in the Plugin Management section of the *USM Appliance Deployment Guide*.

- From the **Taxonomy** page view, you can view and edit the USM Appliance taxonomy (and add new categories and subcategories), which provides a hierarchical arrangement of attack method categories and subcategories (also referred to as event types and sub-types), and their associated data sources, by which policies can match events.

For more information on the USM Appliance event type taxonomy, see [Policy Conditions](#).

- From the **Knowledge Base** page view, you can view and edit articles (documents), and add new articles (documents) to the AlienVault knowledge base. The knowledge base lists known and possible attack events, provides a thorough description of each attack, and describes methods of detection, analysis, and remediation that might be implemented as part of an organization's incident response process to counter an attack.

For more information about the AlienVault Knowledge base, see [Knowledge DB](#).

The Open Threat Exchange (OTX) Page Display

OTX is an open information-sharing and analysis network that provides access to real-time information about issues and attack threats that may impact your organization, allowing you to learn from and work with others who have already experienced such attacks. AT&T Alien Labs™ and other security researchers constantly monitor, analyze, reverse engineer, and reports on sophisticated threats including malware, botnets, phishing campaigns, and more.

When you select the **Configuration > Open Threat Exchange** option, USM Appliance displays the following page.

OPEN THREAT EXCHANGE

OTX Account
ACTIONS ▾

OTX Key:	b67caf33fd9040940346fd1198a5b30b12a81156d99b9eea0cbbb27f00218e	Contribute to OTX:	<input checked="" type="checkbox"/>
OTX Username:	qa	Last Updated:	2016-09-25 14:18:43

OTX Subscriptions (556)

Marsjoke Ransomware Mimics CTB-Locker

2016-09-23 18:52:25 by AlienVault

Ransomware in its various forms continues to make headlines as much for high-profile network disruptions as for the ubiquity of attacks among consumers. We recently noted the non-linear growth of ransomware variants and now a new type has emerged, dubbed Marsjoke. Proofpoint researchers originally spotted the Marsjoke ransomware in late August [1] by trawling through our repository of unknown malware. However, beginning on September 22, 2016, we detected the first large-scale email campaign distributing Marsjoke. This ongoing campaign appears to target primarily state and local government agencies and educational institutions in the United States. The targeting of state and local government agencies as well as the distribution methods are very similar to a CryptFile2 campaign we described in August [2]. Gary Warners's blog also reported on this and similar campaigns, indicating that a well-known botnet, Kelihos, is responsible for distributing this spam [4][5][6].

VIEW IN OTX

MARSJOKE
RANSOMWARE
CTB-LOCKER
MALWARE
PROOFPOINT

ZEUS DELIVERED BY DELOADER TO DEFRAUD CUSTOMERS OF CANADIAN BANKS

2016-09-22 11:12:58 by AlienVault

Throughout September 2016 we have observed an actor sending malware to Canadian nationals by e-mail. Upon investigation we have determined the malware payload to be DELoader, which downloads a Zeus variant banking trojan upon execution.

VIEW IN OTX

ZEUS
DELOADER
JSCRIPT
CANADA
BANKER
FORCEPOINT

The **Configuration > Open Threat Exchange** page provides options to manage your OTX subscription account and OTX keys, and displays a listing of descriptions of the most current threats or attacks that are affecting IT organizations around the world. For each threat description, the abstract also provides tag (keyword) links you can click on to view related OTX pulses that are related to the same threat. In addition, you can click the **View In OTX** button to open (on a separate page) a more detailed description of the threat that includes reference links and groups, statistics and metrics, and Indicators of Compromise (IoC) for the threat. From the list of IoCs displayed for a threat, you can also click on an individual indicator of compromise to see more information about analysis of the threat, and how to detect and identify an attack if it is attempted in your network environment.

Asset Management

Proper asset management is necessary to make the most of the AlienVaultUSM Appliance experience. Asset management allows you to configure USM Appliance according to your needs.

In USM Appliance, asset management includes the following aspects:

- **Asset Discovery**

One of the essential security capabilities that AlienVaultUSM Appliance offers. This capability allows users to discover and inventory all the assets in a network and to correlate asset information with threat and vulnerability data. This functionality uses active and passive network asset scanning.

- **Adding/Deleting assets**

You can add or delete assets manually. See [Adding Assets](#).

- **Vulnerability Scanning**

Vulnerability assessment is another essential security capability that USM Appliance provides. With the asset-oriented security approach introduced in USM Appliance, you can schedule vulnerability scans directly from the assets. See [Running Vulnerability Scans from Assets](#).

- **HIDS Agent Deployment**

Starting with USM Appliance version 5.1, you can deploy HIDS agents directly while managing the assets. See [Deploying HIDS Agents](#).

- **Categorization**

You can categorize your assets in many different ways by using filters or labels.

- **Prioritization**

Not all assets have the same significance. You can prioritize your assets by assigning different values to them. See [Assets and Groups](#).

- **Monitoring assets**

USM Appliance allows two types of asset monitoring: *host monitoring* and *services monitoring*. Host monitoring reports if an asset is up or down, while services monitoring discovers services on an asset and monitors availability of those services.

- **Analysis**

It is essential to investigate the alarms. This may, for instance, require knowing the software version installed on an asset; the existing vulnerabilities; the users who have access to (or traffic generated by) an asset.

This section covers the following subtopics:

Assets and Groups	71
Adding Assets	74
Asset Administration	86
Asset Group Administration	108
Network Administration	114
Network Group Administration	118

Assets and Groups

It is important for security practitioners to know what assets are connected on the company network and how the devices are configured.

What Is an Asset?

In USM Appliance, an asset is a piece of equipment on the company's network that bears a unique IP address. An asset can be a server, a router, a firewall, a printer, a PC or any other network-enabled device.

An asset is monitored by at least one USM Appliance Sensor.

See [Adding Assets](#) or [Asset Administration](#).

Asset Value and Event Risk Calculation

In USM Appliance, every asset or network has an asset value, ranging from 0 to 5, 0 being the least important and 5 the most important. To decide the asset value, the system first checks if a value has been manually assigned. If not, the system uses the asset value of the network the asset belongs to instead. If the network does not have an asset value, USM Appliance assigns the asset the default value of 2. You can assign a different value from the default of 2 to an asset, from 0 to 5.



Important: Keep in mind that raising the value of an asset, which increases the risk of the events, will generate a larger number of false positive alarms, especially when you use the value of 5.

USM Appliance uses asset value to calculate event risk. USM Appliance calculates risk value for every event after it arrives at the USM Appliance Server. The system uses the following formula to calculate the risk:

$$\text{Risk} = (\text{asset value} * \text{event priority} * \text{event reliability}) / 25$$

Where:

- Asset value is from 0 to 5.
- Event priority is from 0 to 5.
- Event reliability is from 0 to 10.

Therefore, the risk value is from 0 to 10. Decimals are always rounded down. For example, if the asset value is 3, event priority is 3, and event reliability is 5, you will get $3 * 3 * 5 / 25 = 1.8$. In this case, the risk for the event is 1.

In USM Appliance, any event with a risk value greater than or equal to 1 generates an alarm.

AlienVault recommends that you do not change the asset value of the USM Appliance instance, because USM Appliance generates its own events, most of which are informational. Therefore, raising the value of this asset (which increases the risk of those events) will generate a larger number of false positive alarms.

Asset Updates

Asset details can be updated by various services in USM Appliance. See the table below for a list of such services. You can also update assets manually by navigating to an asset and selecting **Actions > Edit**. Manual updates can be locked by going to the **Edit Assets > Properties** page. The update with the highest priority number takes precedence over the others, so an update created by a Vulnerability Scan (with a priority of 5) won't overwrite the updates made by an Active Asset Scan (with a priority of 7), but the Vulnerability Scan would overwrite a Passive Asset Scan because it has a lower priority of 4.

Update Priority

Service Name	Priority
Manual — Locked	10
Availability Monitoring	8
LDAP	8
Active Asset Scan	7
WMI	7
Vulnerability Scan	5
HIDS	5
Passive Asset Scan	4
Manual	3

What Are External Assets?

USM Appliance uses External Assets to provide a way for you to create policies and correlation directives on assets that do not belong to you. For example, if a known malicious IP attacks your network, you can add it as an external asset, then create a policy to send out email alerts if this IP communicates to any devices on your network.



Note: Be aware that if you are using an asset-based license, external assets count toward your asset license limit.

When processing events, the correlation engine views external assets or networks as being outside your home network.

What Is an Asset Group?

An asset group is an administratively created object that pools similar assets used for specific purposes. You can group assets based on IP addresses and networks monitored by USM Appliance. Grouping based on IP addresses allows for easier search and management of assets.

For example, you could group all network firewalls, or all servers running a particular operating system. Such groups are useful when performing various tasks, such as vulnerability assessment or asset discovery, or when you are interested only in events coming from specific devices.

You can group assets based on a number of attributes, including the following:

- Asset value
- Network
- Software running on the assets
- Sensor monitoring the assets
- Device type of asset
- Open port or services running on assets
- Location of assets

See [Asset Group Administration](#).

What Is a Network?

In USM Appliance, a network represents a configuration object that identifies the part of an organization's network that USM Appliance monitors. For example, you can select a network during asset discovery to find all the assets on that particular network.

By default, USM Appliance comes with three networks already specified:

- Pvt_192—192.168.0.0/16
- Pvt_172—172.16.0.0/12
- Pvt_010—10.0.0.0/8

See [Network Administration](#).

What Is a Network Group?

Just like an asset group, a network group pools networks with similar properties for easy access and management.

See [Network Group Administration](#).

Adding Assets

USM Appliance provides different ways to add your assets:

- [Adding Assets by Using the Getting Started Wizard](#)
- [Adding Assets by Scanning for New Assets](#)
- [Adding Assets by Importing a CSV File](#)
- [Adding Assets by Using SIEM Events](#)
- [Adding Assets Manually](#)



Note: The USM Appliance system inserts new assets automatically if they are identified through passive asset monitoring, vulnerability scans (if and when vulnerabilities are found), or through IDM events.

Adding Assets by Using the Getting Started Wizard

The Getting Started Wizard is available on USM Appliance All-in-One during the initial setup. This wizard includes the initial tasks for getting AlienVault USM Appliance ready for deployment. As a result, the wizard collects as much data as possible to analyze and identify threats in your environment. One of these tasks is to discover assets using a network scan through the following methods:

- Scanning networks configured in a previous step of the wizard.
- Scanning networks imported from a CSV file.
- Scanning networks added manually.
- Importing assets from a CSV file.
- Adding assets manually.

For more information, see the Getting Started Wizard section in the *USM Appliance Deployment Guide*.

Adding Assets by Scanning for New Assets

This option scans the network for unidentified assets, and adds them to the USM Appliance database so that USM Appliance can monitor them. You can choose to scan an asset, a few assets, an asset group, a network, or a network group. You can run the scan manually or with a schedule:

- [Running a Scan for New Assets Manually](#)
- [Scheduling an Asset Discovery Scan](#)
- [Excluding Assets in an Asset Scan](#)

Running a Scan for New Assets Manually

To run a scan for new assets manually

1. Go to **Environment > Assets & Groups > Assets**.
2. Click **Add Assets**, in the upper right-hand corner, and then **Scan For New Assets**.
3. Select the assets you want to scan:
 - Click the **+** sign to expand the branches in the **All Assets** tree and click your selection.
 - Alternatively, type the name of a specific asset/network in the search box, then press **Enter**.

The selected asset appears in the text field on the left.

4. Select a sensor.
 - **Local** means that USM Appliance uses the sensor on the All-in-One, and **Automatic** means that USM Appliance uses the first sensor available.
 - Alternatively, click **Select a Specific Sensor** to display a list of sensors, choose one from the list.
5. Select the Advanced Options according to your network capacity.

Advanced options for asset scans

Advanced Options	Suboption	Description
Scan Type	Ping	Sends a ping to each asset.
	Fast Scan	(Default) Scans the most common 100 ports.
	Normal	Scans the most common 1000 ports.
	Full Scan	Scans all ports. It can be slow.
	Custom	Allows the user to define the ports to scan.
Timing Template	Paranoid	Scans very slowly. It serializes all scans (no parallel scanning) and generally waits at least 5 min. between sending packets.
	Sneaky	Similar to paranoid mode, but it only waits 15 s between packet transmissions.
	Polite	Eases the network load and reduces the chance of system failure. It serializes the probes and waits at least 0.4 s to send the next probe.
	Normal	(Default) Scans at a rate that achieves the fastest scan throughput without overloading the network or missing hosts and ports.
	Aggressive	Adds a 5-min. timeout per host. Probe response intervals last no longer than 1.25 s.
Autodetect Services and Operating System	None	Only suitable for very fast networks unless you do not mind losing some information.
		Times out hosts in 75 s. Waits only 0.3 s for individual probes. Permits very fast network sweeps.

Advanced options for asset scans (Continued)

Advanced Options	Suboption	Description
Enable Reverse DNS Resolution	None	Determines the domain names associated with the discovered IP addresses, normally against responsive (online) hosts only. Enabled by default.
Privileged Mode	None	Runs asset scans assuming root privileges on Linux/UNIX systems to perform raw socket sends, packet sniffing, and similar operations. This option is enabled by default if you select the Normal, Full Scan, or Custom scan type, or if the Autodetect Services and Operation System option is enabled.

- Click **Start Scan**.

After it completes, the scan result displays in the same page below the Start Scan button.

- Click **Update Managed Assets** to save assets.

USM Appliance adds new assets and updates the existing ones if some of the properties have changed.

Field descriptions for asset scan results

Column/Field Name	Description
<input type="checkbox"/>	Check box to select hosts.
Host	The IP address that identifies the host.
Hostname	The name that identifies the host.
FQDN	Fully Qualified Domain Name of the host.
Device Types	Type of device that identifies the host.
MAC	MAC Address assigned to the host.
OS	Operating System of the host.
Services	The names of the services detected on the host.
FQDN as Hostname	Choose this option to use FQDN as the hostname for the discovered assets. If a FQDN contains any dot, only the name before the first dot is used.

Scheduling an Asset Discovery Scan

You can schedule a scan to run at a set frequency. This is particularly useful on an active network.

To schedule a new asset scan

1. Go to **Environment > Assets & Groups > Schedule Scan > Asset Discovery Scan**.
2. Click **Schedule New Scan** towards the right.
3. Type a name for the new scan.
4. Type the target network or networks to scan. You can type a unique CIDR ($x.x.x.x/xx$) or a CIDR list separated by commas, CIDR1, CIDR2, CIDR3, ..., up to 14 addresses.



Warning: You will not be able to save the scan if you try to add more than 14 CIDR addresses.

5. Select a sensor from the list.
6. Select the advanced options according to your network capacity. For a description of these options, see [Advanced options for asset scans](#).
7. Select scan frequency. The options are **Hourly**, **Daily**, **Weekly** or **Monthly**.

The next scan runs an hour, a day, a week, or a month, respectively, after the previous scan has finished.

8. Click **Save**.



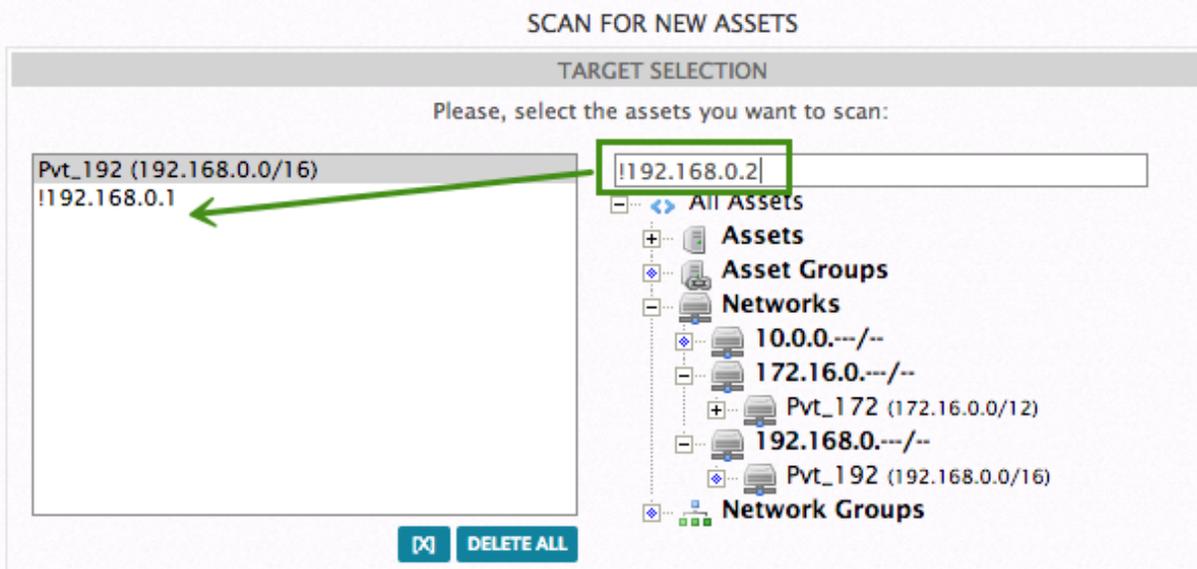
Note: The results of scheduled asset discovery scans do not appear in the web interface. USM Appliance adds the new assets automatically and updates existing ones if it identifies any new properties.

Excluding Assets in an Asset Scan

Occasionally you may want to exclude certain assets such as a printer or a switch when scanning a network. In USM Appliance 5.3.5 and later, you can exclude an asset by putting an exclamation mark ("!") in front of the IP address when configuring a scan.

The following screenshots show an example of excluding $192.168.0.1$ and $192.168.0.2$ while scanning the $192.168.0.0/16$ network.

Example: Excluding assets from a manual asset scan:



Example: Excluding assets from a scheduled asset scan:

Name *

test

Targets to scan *

192.168.0.0/16, !192.168.0.1/32, !192.168.0.2/32

Adding Assets by Importing a CSV File

AlienVaultUSM Appliance allows users to import assets from a CSV file. The allowed formats consist of the following:

```
"IPs (IP1, IP2, ...)"*; "Hostname"; "FQDNs (FQDN1, FQDN2, ...)"*; "Description"; "Asset Value"; "Operating System"; "Latitude"; "Longitude"; "Asset ID"; "External Asset"; "Device Types (Type1, Type2, ...)"
```

Where:

- Delimiter is a semicolon.
- The IPs field is mandatory.
- Hostname syntax is defined by RFC 1123.
- FQDN syntax is defined by RFC 1035, RFC 1123, and RFC 2181.

- Valid operating system values include: Windows, Linux, FreeBSD, NetBSD, OpenSD, MacOS, Solaris, Cisco, AIX, HP-UX, Tru64, IRIX, BSD/OS, SunOS, Plan9, or iOS
- The Asset ID field can be left blank. USM Appliance imports the asset and assign it a new asset ID. If you provide an asset ID and the asset already exists in the system, USM Appliance will update this asset with the values in your CSV file.
- Device types follows this syntax: `Device Category:Device Type`. For example, if you are importing a network router, the value for the device type field should be `Network Device:Router`.

USM Appliance accepted device types

Device Categories	Device Types for
Network Device	Network Device : Bridge Network Device : Broadband Router Network Device : Firewall Network Device : Hub Network Device : Load Balancer Network Device : Remote Management Network Device : Router Network Device : Switch Network Device : Storage Network Device : VPN device Network Device : VPN Gateway (added in version 5.2.2) Network Device : Wireless AP
Endpoint	Endpoint : Endpoint (Other) (added in version 5.2.2) Endpoint : Laptop (added in version 5.2.2) Endpoint : Workstation (added in version 5.2.2)
General Purpose	N / A

USM Appliance accepted device types (Continued)

Device Categories	Device Types for
Industrial Device	Industrial Device : PLC
Media Device	Media Device : Game Console Media Device : IoT Device (Other) (added in version 5.2.2) Media Device : Set Top Box (added in version 5.2.2) Media Device : Television (added in version 5.2.2)
Medical Device (added in version 5.4)	Medical Device : High Priority Medical Device : Other
Mobile	Mobile : Mobile Mobile : Tablet Mobile : PDA Mobile : VoIP Phone
Peripheral	Peripheral : Camera Peripheral : Environmental Monitoring (added in version 5.2.2) Peripheral : IPMI (added in version 5.2.2) Peripheral : Peripheral (Other) (added in version 5.2.2) Peripheral : Power Distribution Unit (PDU) (added in version 5.2.2) Peripheral : Printer Peripheral : RAID (added in version 5.2.2) Peripheral : Terminal Peripheral : Uninterrupted Power Supply (UPS) (added in version 5.2.2)

USM Appliance accepted device types (Continued)

Device Categories	Device Types for
Security Device	Security Device : Antivirus (added in version 5.2.2) Security Device : DDOS Protection (added in version 5.2.2) Security Device : Firewall (added in version 5.2.2) Security Device : Intrusion Detection System Security Device : Intrusion Prevention System Security Device : Network Defense (Other) (added in version 5.2.2) Security Device : Web Application Firewall (added in version 5.2.2)

USM Appliance accepted device types (Continued)

Device Categories	Device Types for
Server	<p>Server : Active Directory Server / Domain Controller (added in version 5.2.2)</p> <p>Server : Application Server (added in version 5.2.2)</p> <p>Server : Backup Server (added in version 5.4)</p> <p>Server : Database Server (added in version 5.2.2)</p> <p>Server : DHCP Server (added in version 5.4)</p> <p>Server : DMZ Server (added in version 5.4)</p> <p>Server : DNS Server</p> <p>Server : Domain Controller</p> <p>Server : File Server</p> <p>Server : HTTP Server</p> <p>Server : Internal Server (added in version 5.4)</p> <p>Server : Mail Server</p> <p>Server : Monitoring Tools Server (added in version 5.2.2)</p> <p>Server : Payment Server (ACI in particular) (added in version 5.2.2)</p> <p>Server : PBX</p> <p>Server : Point of Sale Controller (added in version 5.2.2)</p> <p>Server : Print Server</p> <p>Server : Proxy Server</p> <p>Server : Server (Other) (added in version 5.2.2)</p> <p>Server : Terminal Server</p> <p>Server : Time Server (added in version 5.2.2)</p> <p>Server : Virtual Host (added in version 5.2.2)</p>
	Server : Webserver (added in version 5.2.2)

Each CSV file must contain a header row:

```
"IPs";"Hostname";"FQDNs";"Description";"Asset Value";"Operating System";"Latitude";"Longitude";"Asset ID";"External Asset";"Device Type"
```

For example, with the file below, you add a host with the IP address of 192.168.10.3:

```
"IPs";"Hostname";"FQDNs";"Description";"Asset Value";"Operating System";"Latitude";"Longitude";"Asset ID";"External Asset";"Device Type"
"192.168.10.3";"Host1";"www.example -1.es,www.example -2.es";"This is a test server."; "2";"Windows";"23.78";"121.45";"379D45C0BBF22B4458BD2F8EE09ECCC2";0;"Server:Mail Server"
```

To add assets by using a CSV file

1. Go to **Environment > Assets & Groups > Assets**.
2. Click **Add Assets** at the upper right-hand corner and then **Import CSV**.
3. Click **Choose File** and select a CSV file. If you have special characters in the hostnames and want to ignore them, click the square next to **Ignore invalid characters (Hostnames)**.
4. Click **Import**.

After it finishes, the result page shows the number of assets imported, plus the number of errors and warnings that occurred during the import. You also see an import status summary on every line of the CSV file.

5. To see the details on an error or a warning, click the  icon.
6. To import more assets, click **New Importation**; alternatively, to close the window, click the  icon located at the upper right-hand corner.

Adding Assets by Using SIEM Events

Sometimes new hosts appear in the SIEM events that USM Appliance detects. You can import these hosts as new assets. This option checks events and networks then imports automatically all assets that are found.

To add assets discovered in SIEM events

1. Go to **Environment > Assets & Groups > Assets**.
2. Click **Add Assets** at the upper right-hand corner and then **Import from SIEM**.

The Import Assets from SIEM Events message displays. It shows the number of assets

found.

3. Click **View Log** if you want to read the log file.
4. Click **Import** to transfer the identified assets.

 **Note:** USM Appliance can only import 25,000 assets at a time. Therefore, if you have more than 25,000 hosts, repeat the steps until you have imported all assets.

Adding Assets Manually

USM Appliance also allows you to add an asset manually. This feature helps when you only have a few assets to add, and when you already know the IP addresses of the assets.

While naming an asset in USM Appliance, keep the following rules in mind that an asset name

- Cannot contain any dot (.).
- Cannot start or end with a dash (-).
- Cannot contain a space.
- Can start or end with a letter or a number.
- Can only contain up to 63 characters.

To add assets manually

1. Go to **Environment > Assets & Groups > Assets**.
2. Click **Add Assets** at the upper right-hand corner, and then **Add Host**.
3. On the New Asset page, fill out the fields.
4. Click **Save**.

The Asset Detail page for this asset displays.

Field descriptions for the New Asset and the Asset Details pages

Column / Field Name	Required or Optional	Description
Name	Required	Name of the asset.
IP Address	Required	IP address for the asset.
FQDN/Aliases	Optional	Domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS).

Field descriptions for the New Asset and the Asset Details pages (Continued)

Column / Field Name	Required or Optional	Description
Asset Value	Required	Value assigned to the asset. For further information, see Asset Value and Event Risk Calculation .
External Asset	Required	Whether the asset is on your company network (internal) or not (external). See What Are External Assets? .
Sensors	Required	A list of USM Appliance Sensors with a check mark next to the one monitoring this asset.
Operating System	Optional	Operating System on the asset.
Description	Optional	A short description for the asset.
Icon	Optional	Provide an image for the asset, if desired. The accepted image size is 400 x 400 and the allowed formats are .png, .jpg or .gif.
Location	Optional	Location of the asset. The written location appears on the map. You can also use latitude and longitude to locate the place.
Model	Optional	Model that identifies the asset.
Device Types	Optional	Device type of the asset. Select an option from the Devices list to review options in the Types list. The options are the same as in USM Appliance accepted device types .

Asset Administration

Managing assets occurs in USM Appliance in the Asset List View.

This section covers the following subtopics:

- [Adding Assets](#)
- [Asset List View](#)
- [Searching for Assets](#)
- [Selecting Assets in Asset List View](#)
- [Running Asset Scans](#)

- Running Vulnerability Scans from Assets
- Configure Availability Monitoring
- Viewing Asset Details
- Deleting the Assets
- Editing the Assets
- Exporting the Assets
- Labeling the Assets

Asset List View

The Asset List view, **Environment > Assets & Groups > Assets**, provides a centralized view of your assets.

ASSETS & GROUPS

ASSETS ASSET GROUPS NETWORKS NETWORK GROUPS SCHEDULE SCAN

Search

Assets Search Box

Asset Value: 0 - 1 x

ADD ASSETS -

Export Button

ADD ASSETS -

3 Assets

Clear All Filters

20 ASSETS

Labels Button

ACTIONS -

HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
AV-Windows	172.16.100.2		Microsoft Windows	0	No	Not Deployed
<input checked="" type="checkbox"/> AV-Printer	172.16.100.5		Microsoft Windows	0	No	Not Deployed
<input type="checkbox"/> AV-Console	172.16.100.12		Canonical Ubuntu Linux 14.04 LTS (Long-Term Support)	0	No	Not Deployed

SHOWING 1 TO 3 OF 3 ASSETS

< PREVIOUS 1 NEXT >

Filters

Table of Assets

© COPYRIGHT 2015 ALIENVAULT, INC. | LEGAL

Asset List field descriptions

Column / Field Name	Description
Hostname	Name of the asset.
IP	IP address for the asset.
Device Type	Device type of the asset.
Operating System	Operating System on the asset.
Asset Value	Asset value assigned to the asset.
Vuln Scan Scheduled	Whether a vulnerability scan has been scheduled and enabled.
HIDS Status	The HIDS status for the asset (Connected, Disconnected or Not Deployed).
	Opens the detail page of the asset.

Clicking on an asset displays the status summary of this asset.

Assets ADD ASSETS

Availability Status: Up Has Alarms Has Events

3 Assets

[Clear All Filters](#)

20 ASSETS ACTIONS

<input type="checkbox"/>	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS	
<input type="checkbox"/>	Host-5-9-212-23	5.9.212.23	Server:HTTP Server...	unknown:unknown	2	Yes	Not Deployed	
<input type="checkbox"/>	Host-5-9-212-26	5.9.212.26	Mobile:Tablet	Windows	2	Yes	Not Deployed	

75
Vulnerabilities

33
Alarms

12
Events

UP
Availability

0
Services

1
Groups

1
Notes

<input type="checkbox"/>	usm44	127.0.0.1	Mobile:Tablet	Debian GNU/Linux 6.0.10_2.6.32-5-amd64	2	Yes	Not Deployed	
--------------------------	-------	-----------	---------------	--	---	-----	--------------	--

SHOWING 1 TO 3 OF 3 ASSETS < PREVIOUS 1 NEXT >

Asset status circle color definitions

Type	Color	Description
Vulnerability	Gray	No vulnerabilities.
	Green	Contains Info level vulnerabilities.
	Yellow	Contains one or more <small>Low</small> and/or <small>Medium</small> vulnerabilities.
	Red	Contains one or more <small>Serious</small> and/or <small>High</small> vulnerabilities.
Alarm	Gray	No open alarms on this asset.
	Yellow	Contains open alarms with risk between 1 and 5.
	Red	Contains open alarms with risk greater than 5.
Events	Gray	No events for this asset.
	Yellow	Contains low and/or medium risk events.
	Red	Contains high risk events.
Availability	Gray	Availability status of this asset is not enabled or pending.
	Green	The asset is up.
	Yellow	The asset is unreachable.
	Red	The asset is down.
Services	Gray	Availability monitoring has not been enabled or is pending for one or more services on this asset.
	Green	75%-100% of the ports/services on this asset are available.
	Yellow	One or more services on this asset have an unknown status.
	Red	A Critical or Warning status exists on one or more services on this asset.
Groups	Gray	Displays the number of groups the asset belongs to.
Notes	Gray	Displays the number of notes this asset has.

Searching for Assets

You can either search for or filter your assets by simply typing what you are looking for in the search box, in the upper left-hand corner of the Asset List view. (For UI definitions, see [Asset List View](#).)

The system searches on different fields depending on what you enter:

- If you enter text, USM Appliance searches hostname and FQDN.
- If you enter an IP address, USM Appliance searches the IP, as well as the CIDR.

The result of your search displays with the number of assets identified.

The screenshot shows the 'Assets' page with two filters applied: 'Asset Value: 0 - 1' and 'Last Updated: Last Week'. A green arrow labeled 'Filters' points to these filter boxes. To the right, a box displays 'Number of Assets' as '3 Assets', with a green arrow pointing to it. Below the filters is a table with columns: HOSTNAME, IP, DEVICE TYPE, OPERATING SYSTEM, ASSET VALUE, VULN SCAN SCHEDULED, and HIDS STATUS. The table lists three assets: AV-Windows (IP 172.16.100.2), AV-Printer (IP 172.16.100.5), and AV-Console (IP 172.16.100.12). A green arrow labeled 'Result of the search' points to the table. The page also shows '20 ASSETS' per page, 'SHOWING 1 TO 3 OF 3 ASSETS', and 'Clear All Filters'.

USM Appliance provides a large selection of filters, so that you can find assets easily.

Asset filter in the asset list view

Filter Name	Description
Has Alarms	Identify assets with open alarms.
Has Events	Identify assets with events.
Vulnerabilities	Identify assets with vulnerabilities of all severity levels: Info, Low, Medium, High and Serious. Slide the bar to exclude one or more levels.
Asset Value	Identify assets with a specific asset value, from 0 to 5. Slide the bar to exclude one or more values.

Asset filter in the asset list view (Continued)

Filter Name	Description
HIDS Status	Identify assets with different HIDS connection status. Includes <code>Connected</code> , <code>Disconnected</code> and <code>Not Deployed</code> .
Availability Status	Identify assets with different availability status. Includes <code>Up</code> , <code>Down</code> , and <code>Unconfigured</code> .
Show Assets Added	Identify assets based on date added.
Last Updated	Identify assets based on last date updated.
More Filters	Contains additional filters including <code>Network</code> , <code>Group</code> , <code>Sensor</code> , <code>Device Type</code> , <code>Service</code> , <code>Operating System</code> , <code>Software</code> , <code>Model</code> , <code>Label</code> , <code>Location</code> , and <code>Plugin</code> . Essentially you can filter on every field that classifies or describes an asset.

When applying filters, the search uses a logical "AND" operator when you use different filters. For example, the following search looks for assets that have alarms and events, which were added during the last day:

The screenshot shows a search bar titled "Assets" containing three filter buttons: "Has Alarms x", "Has Events x", and "Assets Added: Last Day x". Below the buttons, the word "AND" is displayed in green text between the first and second buttons, and between the second and third buttons, indicating that all three conditions must be met.

When you use the same filter multiple times, such as `Network` in the following example, USM Appliance uses the logical "OR" operator instead:

The screenshot shows a search bar titled "Assets" containing five filter buttons: "Has Alarms x", "Has Events x", "Assets Added: Last Day x", "Network: Pvt_010 x", and "Network: Pvt_172 x". Below the buttons, the word "AND" is displayed in green text between the first three buttons, and the word "OR" is displayed in green text between the last two buttons, indicating that the first three conditions must be met, and either of the last two conditions can be met.

Selecting Assets in Asset List View

To select a single asset

- Select the check box to the left of the asset.

To select multiple assets

- Select the check box of each asset that you want to include. You can navigate to the next page and select more assets. USM Appliance preserves the selection on the previous page.

To select all the assets on the same page

- Select the check box in the first column of the header row.

To select all the assets returned from a search or all the assets in the system

1. Select all the assets on the page.

Text similar to the following example appears above the asset table

You have selected 20 assets. Select 43,333 assets.

where 43,333 is the number of assets in the system.

2. To select all the assets, click `Select 43,333 assets`.

Assets ADD ASSETS ▾

43,333 Assets

[Clear All Filters](#)

20 ▾ ASSETS You have selected 20 assets. [Select 43,333 assets](#). ACTIONS ▾

<input checked="" type="checkbox"/>	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	AVAILABILITY CONFIGURED	
<input checked="" type="checkbox"/>	AV-Console	172.16.100.12		Canonical Ubuntu Linux 14.04 LTS (Long-Term Support)	0	No	No	
<input checked="" type="checkbox"/>	AV-Firewall	172.16.100.7		Cisco CiscoWorks Windows_WUG	5	No	No	
<input checked="" type="checkbox"/>	AV-IPS	172.16.100.11		Microsoft Windows	4	No	No	
<input checked="" type="checkbox"/>	AV-Mobile	172.100.16.8		Apple Mac OS 9	2	No	No	
<input checked="" type="checkbox"/>	AV-Printer	172.16.100.5		Microsoft Windows	0	No	No	
<input checked="" type="checkbox"/>	AV-Proxy	172.16.100.9		Microsoft Windows	4	No	No	
<input checked="" type="checkbox"/>	AV-Router	172.16.100.6		Cisco Adaptive Security Appliance (ASA) Software 7.0	4	No	No	

Deploying HIDS Agents

In this section, you will learn about deploying HIDS agents from the asset list view:

- [Deploying HIDS Agents to Linux Hosts](#)
- [Deploying HIDS Agents to Windows Hosts](#)
- [HIDS Agent Deployment on Selected Assets](#)
- [Bulk Deployment Constraints](#)
- [Re-naming an Asset with a HIDS Agent Deployed](#)
- [About Legacy HIDS Agents](#)

Deploying HIDS Agents to Linux Hosts

The Asset List View only supports deployment to Microsoft Windows servers. To deploy HIDS agents on Linux hosts, see "Deploying the AlienVault HIDS Agents to Linux Hosts" in the IDS Configuration section of the *USM Appliance Deployment Guide*.

Deploying HIDS Agents to Windows Hosts

Before you can deploy a HIDS agent to the Windows machine, make sure that it meets the following requirements.

- If using any network accelerator devices in the environment, you must add USM Appliance Sensor to their allowlist. This is because the USM Appliance Sensor utilizes SMB (Server Message Block) to transfer the HIDS agent installation package to the Windows machine. If the network accelerator tries to optimize the traffic from the USM Appliance Sensor, it may cause the HIDS deployment to fail.
- The operating system must be one of the following
 - Microsoft Windows XP
 - Windows 7, 8, or 10
 - Windows Server 2003, 2008R2, or 2012R2
- You need to use a user account that belongs to the same Administrators group as the local Administrator account.



Note: For security reasons, the local Administrator account is disabled by default on all versions of Windows currently in mainstream support. In order for the HIDS deployment to succeed, you need to enable the local Administrator account (not recommended), or create a user account and add it to the built-in Administrators group.

- You must have changed the target Windows machine based on the steps below.

To change the settings on Windows XP

1. Go to **Control Panel > Folder Options > View**.
2. Deselect **Use simple file sharing**.
3. Go to **Control Panel > Windows Firewall > Exceptions**.
4. Select **File and Printer Sharing**.

To change the settings on Windows 7

1. Go to **Control Panel > Folder Options > View**.
2. Deselect **Use Sharing Wizard (Recommended)**.
3. Go to **Control Panel > System and Security > Windows Firewall > Advanced Settings > Inbound Rules**.
4. Enable **File and Printer Sharing (SMB-In)**.
5. Go to **Control Panel > User Accounts > Change User Account Control Settings**.
6. Move the slider to **Never notify**.

To change the settings on Windows Server 2003, 2008 R2, and 2012 R2

1. Go to **Control Panel > Windows Firewall > Advanced Settings > Inbound Rules**.
2. Enable **File and Printer Sharing (SMB-In)**.
3. To allow NTLMv2 security, run gpedit.msc.
4. Go to **Local Security > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** and change these settings.
 - a. **Network Security: Minimum session security for NTLMSP based (including secure RPC) clients**, select
 - Require NTLMv2 session security
 - Require 128-bit encryption
 - b. **Network Security: Minimum session security for NTLMSP based (including secure RPC) servers**, select
 - Require NTLMv2 session security
 - Require 128-bit encryption
 - c. **Network Security: LAN Manager Authentication level**, select
 - Send NTLMv2 response only\refuse LM & NTLM

To change the settings on Windows 8 and 10

1. Go to **Control Panel > Folder Options > View**.
2. Deselect **Use Sharing Wizard (Recommended)**.
3. Go to **Control Panel > System and Security > Windows Firewall > Advanced Settings > Inbound Rules**.
4. Enable **File and Printer Sharing (SMB-In)**.
5. Enable **Windows Management Instrumentation (WMI)** entry.
6. Go to **Control Panel > User Accounts > Change User Account Control Settings**.
7. Move the slider to **Never notify**.
8. Open **Group Policy**.
 - a. Go to **Local Policies > Security Options**
 - b. Set **Network access: Shares that can be accessed anonymously** to `IPC`.
 - c. Set **User Account Control: Run all administrators in Admin Approval Mode** to `Disabled` (recommended).
9. Apply changes and restart the machine.



Note: The Winexe installation utility may trigger a false positive alert as a “potential hacking tool” during an authorized application installation, even though the Winexe remote installation is an authorized action. In this instance, the best practices are to either allowlist the IP address of USM Appliance, or temporarily disable the antivirus software during the installation.

HIDS Agent Deployment on Selected Assets

To deploy HIDS agents on selected assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to edit. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions**, and then **Deploy HIDS Agents**.

The Deploy HIDS Agents screen appears.

4. Type your MS Windows login credentials. Domain is optional, but the user accounts must have administrator privileges.

5. Click **Deploy**.

USM Appliance deploys HIDS agents on the selected asset(s). For every deployment attempt, the system generates a message in the Message Center with the outcome.



Note: After successful deployment, USM Appliance does not show the status of the HIDS agents in real time. Instead, it updates the agents in the background, hourly.

Bulk Deployment Constraints

If you plan to deploy HIDS agents to multiple assets at the same time, keep the following in mind:

- You must be able to access the selected assets using the same credential.
- All of the assets are Windows-based.

If none of the assets are Windows-based, USM Appliance does not deploy the HIDS agents. A warning message displays instead.

If only some of the assets are Windows-based, you have the following options:

- **Cancel.** Cancel the deployment and go back to the [Asset List View](#).
- **View these assets.** Cancel the deployment and view the non-Windows assets in the [Asset List View](#).
- **Continue.** Continue with the deployment on the Windows assets only.

Re-naming an Asset with a HIDS Agent Deployed

You cannot change the name of an asset when the deployed HIDS agent is connected. To update the name properly, you must disconnect the HIDS agent first, or shut it down.

About Legacy HIDS Agents

If you upgrade to USM Appliance version 5.1 from a previous version, you may already have some HIDS agents deployed. USM Appliance tries to link legacy HIDS agents with an asset. If the IP address of the HIDS agent does not exist in the inventory, the system creates a new asset with that IP address.

Should the system not have enough information to link the HIDS agent with an asset, a message appears in the Message Center, asking you to link the asset manually.

To connect an HIDS agent with an asset

1. Go to **Environment > Detection > HIDS > Agents**.

The list of HIDS agents displays.

2. Select the HIDS agent without a value in the **Asset** column and click the link (🔗) icon.

The Connect an Asset to HIDS agent page displays.

3. Type in the IP address of the asset or select it from the asset tree.
4. Click **Save**.
5. Click **Yes** to confirm.

Running Asset Scans

You can run an asset scan on individual assets. This is useful, for example, if you want to find out if anything has changed on these assets.



Note: Before scanning a public network space, see "Addendum Notice Regarding Scanning Leased or Public Address Space" under System Overview in the *USM Appliance Deployment Guide*.

To run asset scan on selected assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to edit. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions**, and then **Run Asset Scan**.

On Asset Scan, it displays the list of assets you selected, the USM Appliance Sensor performing the scan, and the scan status.

Scan status meaning

Icon	Meaning
	The sensor is ready to start the scan.
	The sensor is not connected.

Scan status meaning (Continued)

Icon	Meaning
	The sensor is busy with other scan jobs.

4. Select the advanced options according to your network capacity. For meaning of these options, see [Advanced options for asset scans](#).
5. Click **Start Scan**.

A message displays, informing you that the asset scan has started. If the scan identifies any new assets, USM Appliance adds them to the asset list automatically.

Running Vulnerability Scans from Assets

You can run vulnerability scans on individual assets.

The fewer assets to scan, the sooner the scan finishes.

 **Note:** Before scanning a public network space, see "Addendum Notice Regarding Scanning Leased or Public Address Space" under System Overview in the *USM Appliance Deployment Guide*.

 **Important:** Threat intelligence update will not finish if any vulnerability scan is running, because the update needs to refresh the vulnerability threat database used by the scan.

To run a vulnerability scan on selected assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to edit. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions**, and then **Run Vulnerability Scan**.

On Vulnerability Scan, the selected assets display at the bottom.

4. Identify the scan job by typing a name in the **Job Name** field.
5. Select a sensor from the **Select Sensor** list.

 **Important:** You can only run up to 5 concurrent scans per USM Appliance Sensor.

6. Select a profile from the **Profile** list or create your own scan profile, see [Vulnerability Scan Profiles](#) for descriptions.
7. In **Schedule Method**, do one of the following:
 - To launch the scan without any delay, keep the default value as "Immediately".
 - To schedule the job to run at a different time, make a selection based on the table below.

USM Appliance vulnerability scan schedules

Schedule Method	Description
Immediately	Launch the scan job without any delay.
Run Once	Run scan once at the specified date and time.
Daily	Run scan every x days at the specified time beginning on the specified day.
Day of the Week	Run scan on the specified day and time of the week.
Day of the Month	Run scan on the specified day and time of the month.
Nth week of the month	Run scan on the specified day and time on the Nth week of the month. A week starts on the first day of the month and lasts 7 days.

8. (Optional) Click **Advanced**.
 - For authenticated scans, choose **SSH Credential** (UNIX/Linux) or **SMB Credential** (Windows), depending on the operating system of your hosts.



Note: Skip this step for unauthenticated scans. You need to create the credentials first. For assistance, see [Creating Credentials for Vulnerability Scans](#).

- Specify the maximum time (in seconds) that the scan should run.

In USM Appliance version 5.2 and earlier, the default is 28,800 seconds (8 hours).

In USM Appliance version 5.3 and later, the default is 57,600 seconds (16 hours).

- To **send an email notification** after the scan finishes, select **Yes**, and then select **User** or **Entity** as the email recipient.



Important: Be aware of the following when making the selection:

- Admins can view all scans.
- If you are not an admin and you assign the scan to a different user, you can't view this scan yourself.
- If you are an admin and you don't assign the scan to any user or entity, all non-admin users can't view this scan.
- If you are an admin and you assign this scan to a non-admin user, both you and the non-admin user can view this scan, but other non-admin users can't.
- If you assign the scan to an entity, all users who belong to the entity can view the scan.

See [USM Appliance User Accounts](#) for the definition of different user roles.

9. (Optional, available in USM Appliance version 5.3.2 and later) Specify the port numbers you do not want to scan in **Exclude Ports**. Use comma to separate the port numbers but do not use any space between them. For example, "1,33,555,26-30,44".



Note: Using this option slows down the scan because USM Appliance performs additional tasks to exclude the ports you specify.

10. (Optional) To speed up the scanning process, click **Only scan hosts that are alive**.
11. (Optional) If you do not want to pre-scan from a remote sensor, click **Pre-Scan locally**.
12. (Optional) If you do not want to resolve hostnames or FQDN, click **Do not resolve names**.
13. To create the vulnerability scan, click **Save**.

Configure Availability Monitoring

Availability monitoring in USM Appliance runs from the server, and can be used to monitor availability, assets, and services within your network. Monitoring an asset or service may require for the designated ports and ICMP protocol to be monitored as well. USM Appliance provides two types of asset availability monitoring:

- Host monitoring — reports whether an asset is up or down
- Services monitoring — discovers services on an asset and monitors their availability

You can also enable the AlienVault Availability-Monitoring plugin to see events, see [Enabling Plugins on Assets](#).

To enable availability monitoring on selected assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to label. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions** and then **Enable Availability Monitoring**.

A message displays informing you that the enablement was successful.

4. To see the status of these assets and the services running on them, see the Asset Detail page for the individual asset.

To disable availability monitoring on selected assets

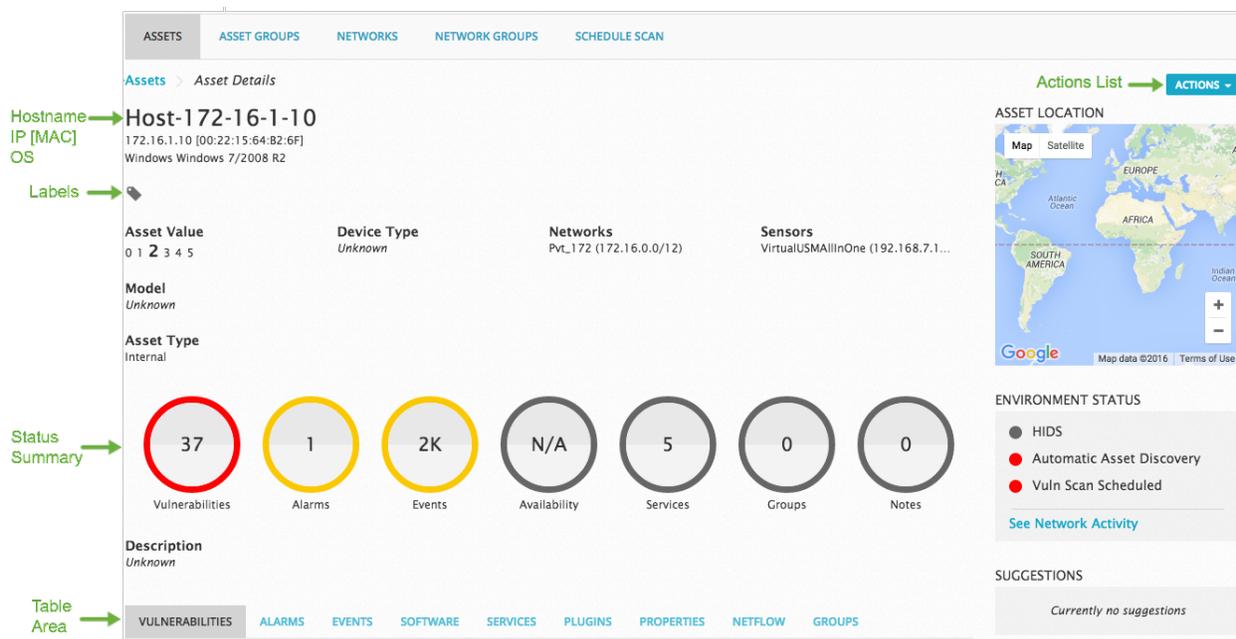
1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to label. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions** and then **Disable Availability Monitoring**.

A message displays informing you that the disabling was successful.

Viewing Asset Details

To view asset details from the Asset List view, double-click a specific asset or click the magnifying glass () icon at the end of the row.

The Asset Details page looks similar to the following:



In Asset Details, on the left, you see the name and IP address, along with other fields that describe the particular asset.

In the middle, you see the status summary for your asset. (See [Asset status circle color definitions](#) for reference.)

At the bottom, you see a table area with tabs that correspond to the circles. Each tab contains a table with records, if present, for your asset. For example, in the figure shown, Host-172-16-1-10 has 37 vulnerabilities. On the Vulnerabilities tab (not shown), you see a table listing the 37 vulnerabilities, one by one.

Asset Details view tab description

Tab	Information Shown
Vulnerabilities	Vulnerabilities related to this asset.
Alarms	Alarms related to this asset.
Events	Events related to this asset.
Software	Software installed on this asset. Use the Edit Software button to add, modify or delete software.
Services	Services available on this asset. Use the Edit Services button to add, modify or delete services. While in Edit Services, you can enable or disable availability monitoring for the service(s).

Asset Details view tab description (Continued)

Tab	Information Shown
Plugins	Plugins enabled for this asset. Use the Edit Plugins button to enable or disable plugins for this asset. You can enable up to 10 plugins per asset and up to 100 plugins per USM Appliance Sensor.
Properties	Properties specified for this asset. Use the Edit Properties button to add, modify or delete properties.
NetFlow	NetFlow information related to this asset.
Groups	Asset groups to which the asset belongs. Use the Add to Group button to add or remove the asset from an asset group.

On the right side of the page, you see a list of **Actions** to perform on this asset. These consist of

- Edit
- Delete
- Run Asset Scan
- Run Vulnerability Scan
- Enable Availability Monitoring
- Disable Availability Monitoring

Asset Location displays a map showing the location of the asset, if set.

The **Environment Status** area displays status of your asset. The circles next to each link appear in different colors, indicating various status.

Environment status colors and meanings for assets

Environment Status	Color	Meaning
HIDS	Green	An HIDS agent is deployed on this asset with status Active or Active/Local.
	Yellow	A HIDS agent is deployed on this asset with status Disconnected.
	Red	A HIDS agent is deployed on this asset with status Never Connected.
	Gray	No HIDS agent is deployed on this asset.

Environment status colors and meanings for assets (Continued)

Environment Status	Color	Meaning
Automatic Asset Discovery	Green	All IP addresses associated with this asset are scheduled to be scanned.
	Yellow	Some IP addresses associated with this asset are scheduled to be scanned.
	Red	No IP addresses associated with this asset is scheduled to be scanned.
Vuln Scan Scheduled	Green	A vulnerability scan has been scheduled for this asset.
	Red	No vulnerability scan has been scheduled for this asset.

To check HIDS status

- Click **HIDS**.

This takes you to **Environment > Detection > HIDS > Overview**, where you see a list of HIDS agents along with their status.

To set up an asset scan

- Click **Automatic Asset Discovery**.

This takes you to **Environment > Assets & Groups > Scheduled Scan**, where you can schedule an asset discovery scan. See [Scheduling an Asset Discovery Scan](#).

To see the vulnerability scan scheduled or to schedule a vulnerability scan

- Click **Vuln Scan Scheduled**.

This takes you to **Environment > Vulnerabilities > Scan Jobs**, where you see a list of vulnerability scan jobs.

To see various network activity on this asset

- Click **See Network Activity**.

This takes you to **Environment > NetFlow > Details**, with the IP address of the asset set as either the source or destination.

The **Suggestions** section displays suggestions USM Appliance provides for the asset. These suggestions can be informative, warning, or error messages.

To see suggestion details

- Click the message.

Deleting the Assets

To delete asset(s)

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to delete. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions** and then **Delete**.

20 ASSETS						ACTIONS	
<input type="checkbox"/>	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCHE	<input type="checkbox"/> Edit <input checked="" type="checkbox"/> Delete
<input type="checkbox"/>	AV-UbuntuLTS	172.16.100.4		Canonical Ubuntu Linux 14.04 LTS (Long-Term Support)	5		<input type="checkbox"/> Run Asset Scan <input type="checkbox"/> Run Vulnerability Scan <input type="checkbox"/> Deploy HIDS Agents <input type="checkbox"/> Enable Availability Monitoring <input type="checkbox"/> Disable Availability Monitoring <input type="checkbox"/> Create/Add To Group <input type="checkbox"/> Add Note
<input type="checkbox"/>	AV-Firewall	172.16.100.7		Cisco CiscoWorks Windows_WUG	5		
<input type="checkbox"/>	AV-Proxy	172.16.100.9		Microsoft Windows	4		
<input type="checkbox"/>	bat50	172.16.100.1		Netgear Netgear WNR3500	4	No	Not Deployed
<input checked="" type="checkbox"/>	AV-Router	172.16.100.6		Cisco Adaptive Security Appliance (ASA) Software 7.0	4	No	Not Deployed
<input type="checkbox"/>	AV-IPS	172.16.100.11		Microsoft Windows	4	No	Not Deployed

Editing the Assets

You can edit your assets once they are in USM Appliance. For example, you can add a description or a location for your asset, or increase the asset value to indicate that certain assets are more important than the others. You can modify the same field or fields for multiple assets at the same time.

To edit your assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to edit. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions** and then **Edit**.

The Edit Assets screen displays.

4. Modify the fields. For field descriptions, see [Field descriptions for the New Asset and the Asset Details pages](#).



Note: In addition to the General tab, you can use the Properties and Software tab, as well.

5. Click **Save**.

A message displays informing you that the system has saved your changes.



Important: All user-defined property values have higher priority than those detected by other USM Appliance tools, such as software inventory, HIDS, and passive or active asset discovery. The AlienVault appliances are recognized as "AlienVault OS".

If you cannot find an appropriate field to use, you can always add a note to the asset.

To add a note to your asset(s)

1. Go to **Environment > Assets & Groups > Assets**.
2. Select one or more assets that you want to edit. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions** and then **Add Note**.

The Add Note screen displays.

4. Type a note and click **Save**.

Exporting the Assets

To export assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to export. For assistance, see [Selecting Assets in Asset List View](#).
3. Click the download icon () on the upper right-hand corner.

Your browser downloads the exported file automatically. The filename has the following structure: Assets__yyyy-mm-dd.csv.

 **Note:** Use semicolons to delimit this exported file.

Labeling the Assets

You can use labels to further classify your assets and later use them when [Searching for Assets](#).

To label your assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to label. For assistance, see [Selecting Assets in Asset List View](#).
3. Click the label icon () towards the right, next to Actions.
4. Select the label you would like to use.

A message displays informing you the number of assets with this label added.

Meaning of the symbols when labeling assets

Symbol	Meaning
	Some of the selected assets currently use this label.
	All of the selected assets currently use this label.
	None of the selected assets currently use this label.

To remove any label from your assets

- Follow the same procedure as above but deselect the label instead.

You can add or remove labels as well.

To manage asset labels

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to label. For assistance, see [Selecting Assets in Asset List View](#).



Note: Even though you are not trying to label any assets for this task, you still need to select at least one asset to activate the label icon.

3. Click the label icon towards the right, next to Actions.

4. Click **Manage Labels**.

The Manage Labels screen displays.

5. To add a new label, provide a **Name**, choose a **Style** for it, then click **Save**.

You will see the label in the Preview area before saving it.

6. Alternatively, click delete icon () to remove a label.

7. Click the X icon () to close the screen.

Asset Group Administration

This section covers the following subtopics:

- [Asset Group List View](#)
- [Creating an Asset Group](#)
- [Viewing Asset Group Details](#)

Asset Group List View

An asset group is an administratively created object that pools similar assets used for specific purposes. USM Appliance provides a centralized view for managing your asset groups. This view is on **Environment > Assets & Groups > Asset Groups**. It has the same look and feel as the asset list view. The difference is that in this view, you manage asset groups instead of assets.

The screenshot shows the 'ASSETS & GROUPS' interface. On the left, there are filter sections for 'Has Alarms', 'Has Events', 'Vulnerabilities', and 'Asset Value'. Below these are 'Show Assets Added' and 'Last Updated' options. A 'MORE FILTERS' button is at the bottom left. The main area is titled 'Asset Groups' and features a search box at the top left. A 'CREATE NEW GROUP' button is at the top right. A summary box shows '2 Groups' and a 'Clear All Filters' link. Below this is a table with columns: NAME, OWNER(S), ASSETS, ALARMS, VULNERABILITIES, and EVENTS. The table lists two groups: 'EventsAlarms' and 'assetValue_4'. To the right of the table are 'Labels Button' and 'Actions Button' (with a dropdown arrow). Below the table, there are 'Modify Button' and 'Details of a Group' icons. The text 'SHOWING 1 TO 2 OF 2 GROUPS' is at the bottom of the table area.

Clicking on an asset group displays the status summary of this group.

The screenshot shows the 'Asset Groups' status summary for the 'cinconueve' group. At the top, there is a 'CREATE NEW GROUP' button and a filter for 'Vulnerabilities: Info - Serious'. A summary box shows '2 Groups' and a 'Clear All Filters' link. Below this is a table with columns: NAME, OWNER(S), ASSETS, ALARMS, VULNERABILITIES, and EVENTS. The table lists two groups: 'cinconueve' and 'local'. Below the table, there is a detailed view of the 'cinconueve' group with seven circular gauges: Assets (23), Vulnerabilities (123), Alarms (9K), Events (30K), Availability (21%), Services (9), and Notes (1). The text 'SHOWING 1 TO 2 OF 2 GROUPS' is at the bottom of the table area.

Asset group status circle color definitions

Type	Color	Description
Assets	Gray	Displays the number of assets in the group.
Vulnerability	Gray	No vulnerabilities.
	Green	Contains Info level vulnerabilities.
	Yellow	Contains 1 or more Low and/or Medium vulnerabilities.
	Red	Contains 1 or more Serious and/or High vulnerabilities.
Alarm	Gray	No open alarms for this asset group.
	Yellow	Contains open alarms with risk between 1 and 5.
	Red	Contains open alarms with risk greater than 5.
Events	Gray	No events for this asset group.
	Yellow	Contains low and/or medium risk events.
	Red	Contains high risk events.
Availability	Gray	Availability status of this asset group is not enabled and/or pending.
	Green	95%-100% of this asset group are available.
	Yellow	75%-95% of this asset group are available.
	Red	Less than 75% of this asset group are available.
Services	Gray	Availability monitoring has not been enabled and/or pending for one or more services.
	Green	75%-100% of the ports/services on this group are available.
	Yellow	One or more services in this asset group has an unknown status.
	Red	A Critical or Warning status exists on one or more services in this asset group.
Notes	Gray	Displays the number of notes on this asset group.



AlienVault OSSIM Limitations: Amazon Web Service and Microsoft Azure asset discovery is only available in USM Appliance.

Creating an Asset Group

In USM Appliance, you can create an asset group in the following ways:

- From the [Asset List View](#), select assets first, and then create the group.
- From the [Asset Group List View](#), create the asset group first, and then add assets to it.



Warning: Asset group names cannot include the following characters:

~!\$%^&*|' "<>?, () =.

To create an asset group from the asset list view

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to group together. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions**, and then **Create / Add to Group**.
4. On Create or Add to Group, do one of the following:
 - a. To create a new group, in the **New Group** field, enter a name for the asset group, then click the plus icon () towards the right.
 - b. To add the selected assets to an existing group, locate the group by its name and click the plus icon in the same row.

The page refreshes and the corresponding Asset Group Details page displays.

CREATE OR ADD TO GROUP ✕

NAME	ACTIONS
PabloOwner	<input style="background-color: #0070c0; color: white; border: none; padding: 2px 5px;" type="button" value="+"/>
localhost	<input style="background-color: #0070c0; color: white; border: none; padding: 2px 5px;" type="button" value="+"/>
local	<input style="background-color: #0070c0; color: white; border: none; padding: 2px 5px;" type="button" value="+"/>
cinconueve	<input style="background-color: #0070c0; color: white; border: none; padding: 2px 5px;" type="button" value="+"/>

SHOWING 1 TO 4 OF 4 ENTRIES < PREVIOUS 1 NEXT >

New Group

To create an asset group from the asset group list view

1. Go to **Environment > Assets & Groups > Asset Groups**.
2. Click **Create New Group** towards the right.
3. Type a name for the asset group. Optionally, provide a description for the group as well.
4. Click **Save**.

The page refreshes and the corresponding Asset Group Details page displays.

5. Click **Add Assets**.

6. On **Add Assets to Group**, click the plus icon on the asset you want to add.

The page displays 10 assets by default, but you can change it to display 20 or 50 assets. Use the **Search** field if you do not see the asset you plan to add.

7. Click the X icon (✕) to exit the page.

The page refreshes and the selected assets display in the **Assets** tab. The first circle shown in **Asset Group Details** view displays the number of assets in this group.

Viewing Asset Group Details

From the **Asset Group List** view, when you double-click a specific asset group, or click the magnifying glass (🔍) icon at the end of the row, the **Asset Group Details** view displays.

The **Asset Group Details** page looks identical to the Asset Details page, except that it contains information for all the assets belonging to this group. You see the number of assets displayed in the status summary, and each asset listed in the **Assets** tab.

The **Environment Status** area displays status in different colors for your asset group.

Environment status colors and meanings for asset groups

Environment Status	Color	Meaning
HIDS	Green	All the assets in this group have HIDS agents deployed and all of them are active.
	Yellow	Some of the assets in this group have HIDS agents deployed but some of them are not active.
	Red	Some of the assets in this group have HIDS agents deployed but they are not connected.
	Grey	None of the assets in this group have HIDS agents deployed.
Automatic Asset Discovery	Green	All the assets in this group are scheduled to be scanned.
	Yellow	Some of the assets in this group are scheduled to be scanned.
	Red	None of the assets in this group are scheduled to be scanned.
Vuln Scan Scheduled	Green	All the assets in this group have a vulnerability scan scheduled.
	Red	None of the assets in this group have a vulnerability scan scheduled.

To export the asset group into a CSV file

- Click the download icon () at the upper right-hand corner.

Your browser downloads the file or prompts you to download it.

The name of the generated file has the following structure: `Assets_from_group_groupID_
_yyyy-mm-dd.csv`.

Network Administration

This section covers the following subtopics:

- [Network List View](#)
- [Creating a Network](#)
- [Viewing Network Details](#)

Network List View

AlienVault USM Appliance provides a centralized view for managing your networks.

It has a similar look-and-feel to the Asset List View. You can perform the same actions on networks as you do on assets, except for the following differences.

- You cannot edit multiple networks at the same time.
- You can run asset scans or vulnerability scans on your network(s), but you cannot enable or disable availability monitoring for a network.

For details, see [Asset Administration](#).

The screenshot displays the 'ASSETS & GROUPS' interface with the 'NETWORKS' tab selected. The interface includes a search box, a filter sidebar on the left, and a table of networks. The table has columns for NETWORK NAME, CIDR, OWNER(S), SENSORS, ALARMS, VULNERABILITIES, and EVENTS. The table shows 5 networks, with the first two selected. The interface also features an 'ADD NETWORK' button, an 'EXPORT' button, and an 'ACTIONS' button. The table is labeled 'Table of Networks' and the filter sidebar is labeled 'Filters'. The 'ACTIONS' button is labeled 'Actions Button' and 'Labels Button'. The 'ADD NETWORK' button is labeled 'Add Network Button'. The 'EXPORT' button is labeled 'Export Button'. The 'DETAILS' icon for the first network is labeled 'Details of a Network'. The 'EDIT' icon for the first network is labeled 'Modify Button'.

NETWORK NAME	CIDR	OWNER(S)	SENSORS	ALARMS	VULNERABILITIES	EVENTS
<input checked="" type="checkbox"/> ADF	10.0.0.0/18		VirtualUSMAllInOne	-	-	-
<input checked="" type="checkbox"/> fdasasd asdf asdf	192.168.0.0/15		VirtualUSMAllInOne	-	-	-
<input type="checkbox"/> Pvt_010	10.0.0.0/8		VirtualUSMAllInOne	✓	-	✓
<input type="checkbox"/> Pvt_172	172.16.0.0/12		VirtualUSMAllInOne	-	-	-
<input type="checkbox"/> Pvt_192	192.168.0.0/16		VirtualUSMAllInOne	-	-	-

Creating a Network

In USM Appliance, you can create a network either manually or by importing a CSV file.

Creating a Network by Importing a CSV File

AlienVaultUSM Appliance allows users to import networks from a CSV file. The allowed formats consist of the following:

```
"Netname"*;"CIDRs (CIDR1,CIDR2,...)"*;"Description";"Asset Value"*;"Net ID"
```

Where:

- The delimiter is a semicolon.
- The Netname, CIDRs, and Asset Value fields are mandatory.
- The Netname field allows these characters: A-Z, a-z, 0-9, ., :, _, and -.

Each CSV file must contain a header row:

```
"Netname";"CIDRs";"Description";"Asset Value";"Net ID"
```

For example, with the file below, you add a network with a CIDR of 192.168.10.0/24 and 192.168.9.0/24:

```
"Netname";"CIDRs";"Description";"Asset Value";"Net ID"
"Net_1";"192.168.10.0/24, 192.168.9.0/24";"This is my
network";"2";"479D45C0BBF22B4458BD2F8EE09ECAC2"
```

To create a network by importing a CSV file

1. Go to **Environment > Assets & Groups > Networks**.
2. Click **Add Network** at the upper right-hand corner, and then **Import CSV**.
3. Click **Choose File** and select a CSV file.

If you have special characters in the file and want to ignore them, click the square next to **Ignore invalid characters**.

4. Click **Import**.

Creating a Network Manually

To create a network manually

1. Go to **Environment > Assets & Groups > Networks**.
2. Click **Add Network** towards the upper right-hand corner, and select **Add Network**.
3. On New Network, fill out the fields.
4. Click **Save**.

The page refreshes and the corresponding Network Details page displays.

Network field descriptions

Column/Field Name	Required or Optional	Description
Name	Required	Name of the network.
CIDR	Required	CIDR (Classless Inter-Domain Routing) for the network.
Owner	Optional	Domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS).
Sensors	Required	A list of USM Appliance Sensors with a check mark next to the one monitoring this network.
Asset Value	Required	Value assigned to the network. For further information, see Asset Value and Event Risk Calculation .
External Asset	Required	Whether the network is on your company network (internal) or not (external). See What Are External Assets? .
Icon	Optional	Provide an image for the network, if desired. The accepted image size is 400 x 400 and the allowed formats are .png, .jpg or .gif.
Description	Optional	A short description of the network.

Viewing Network Details

From the [Network List View](#), you can double-click a specific network or click the view icon () at the end of the row to view Network Details.

The Network Details page looks identical to the [Asset Group Details page](#), except that it contains information for all the assets belonging to this network.

To export the network into a CSV file

- Click the download icon () at the upper right-hand corner.

Your browser downloads the file or prompts you to download it.

The name of the generated file has the following structure: `Networks__yyyy-mm-dd.csv`.

Network Group Administration

- [Network Group List View](#)
- [Managing Network Groups](#)

Network Group List View

From the Network Group List view (**Environment > Assets & Groups > Network Groups**), you can create and manage network groups.

ASSETS & GROUPS ?

ASSETS ASSET GROUPS NETWORKS **NETWORK GROUPS** SCHEDULE SCAN

SHOW ENTRIES NEW MODIFY DELETE SELECTED

NAME	NETWORKS	DESCRIPTION	KNOWLEDGE DB	NOTES
nbm1	Pvt_172			
nbm2	Pvt_192			
nbm3	Pvt_172, Pvt_010			

< PREVIOUS NEXT >

For details about how to create and manage a network group, see [Managing Network Groups](#).

Managing Network Groups

You manage network groups from the Network Group List view.

Creating Network Groups

To create a network group

1. Go to **Environment > Assets & Groups > Network Groups**.
2. Click **New**.
3. Type a name for the new group.

4. Select networks from the network structure or enter a specific one in the Filter box; click **Apply**.

The chosen network appears in the area below.

if you make a mistake, use the Delete () button to remove it.

5. (Optional) Type a description that identifies the network group.
6. Click **Save**.

Editing Network Groups

To edit a network group

1. Go to **Environment > Assets & Groups > Network Groups**.
2. Select the network group and click **Modify**.
3. Make the changes and click **Save**.

Deleting Network Groups

To delete a network group

1. Go to **Environment > Assets & Groups > Network Groups**.
2. Select the group and click **Delete Selected**.

Alarm Management

An alarm in AlienVault USM Appliance consists of one or more events, based on one of the following:

- One or more out-of-the-box directives, or rules, performed by the correlation engine of the USM Appliance Server. These look at and connect *multiple events* to assess their relative priority and reliability. The events then get re-injected into the USM Appliance Server process as though they were coming from the USM Appliance Sensor. For more information about correlation rules, see [Correlation Rules](#).
- Elevated parameters that USM Appliance evaluates, based on existing policy configurations and event risk. An alarm is generated when the risk of an event is ≥ 1 . Because risk is calculated as $\text{Risk} = \text{asset value} * \text{reliability} * \text{priority} / 25$, the likelihood of an alarm will be influenced by the asset or network value. It is important to consider correlation settings in regard to risk values, as you may want multiple directive rules depending on reliability and asset values. For more information about directives, see [Event Correlation](#).

Depending on how your policies are configured, this can account for alarms coming from various sources. For example, policies set up in the **Default policy group** can process alarms from events, while **Policies for events generated in the server** will only target server events. For more information about policy groups, see [The Policy View](#).

- Alarms are generated and processed differently for events related to OTX pulses. For more information, see [Viewing OTX Alarms](#).

This section covers the following subtopics:

Alarms Page Overview	121
Reviewing Alarms as a Group	122
Reviewing Alarms as a List	124
Taking Ownership of an Alarm	136
Back Up and Restore Alarms	138

Alarms Page Overview

When you select the **Analysis > Alarms** option, USM Appliance displays the following page.

The screenshot shows the 'ALARMS' section of the USM Appliance interface. At the top, there are two tabs: 'LIST VIEW' (highlighted with a green box) and 'GROUP VIEW'. Below the tabs is a refresh indicator: 'Next refresh in 127 seconds. Or click here to refresh now'. A 'SEARCH AND FILTER' section contains several dropdown menus for Sensor, Alarm Name / ID, Source IP Address, Destination IP Address, Date, Asset Group, Intent, Directive ID, and Label. There are also checkboxes for 'Only OTX Pulse Activity', 'Do not resolve ip names', 'Hide closed alarms', and 'Beep on new alarm'. A 'SEARCH' button is located below the filters. Below the search filters is a heatmap visualization showing alarm activity over a 31-day period (from 16-09-19 to 16-09-25). The heatmap has five rows representing different alarm types: System Compromise, Exploitation & Installation, Delivery & Attack, Reconnaissance & Probing, and Environmental Awareness. The columns represent days. Blue dots indicate alarm activity, with a large blue circle indicating a high concentration of alarms on 16-09-23. Below the heatmap is a table with columns: SHOW (set to 20), ENTRIES, DATE, STATUS, INTENT & STRATEGY, METHOD, RISK, OTX, SOURCE, and DESTINATION. Two entries are visible in the table:

SHOW	ENTRIES	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
20		3 hours	🔄	🚨 Vulnerable software	Java	LOW (1)	N/A	10.192.72.79:1632	🇺🇸 199.168.151.20:249
20		3 hours	🔄	🚨 Bruteforce Authentication	SSH	LOW (1)	N/A	🇫🇷 139.158.161.108:1111	10.187.166.1:241

By default, the display opens in List View, which simply lists alarms in reverse chronological order (the latest issued alarm is displayed first). You can also change the display to Group View, which allows you to group alarms by different keys such as alarm name, source and destination IP address, or alarm type.

The middle portion of the screen includes a table that provides a graphical aggregated representation of alarms based on directive events, which are events generated by the USM Appliance Server. The table contains such alarms occurred in the last 31 days; each column

represents a different day. Blue circles indicate the number of times that an alarm in a category appeared. A bigger circle indicates a higher number of alarms were generated. You can mouse over each of the circles to get the actual number of different types of alarms that occurred as well as a Top 5 list of possible remedies for each alarm type.

Alarms are sorted into five different categories, which are represented by the graphic icons in the display. These are:

- System compromise ()
- Exploitation and installation ()
- Delivery and attack ()
- Reconnaissance and probing ()
- Environmental awareness ()

The categories are also consistent with the sequence or stages of events that an attacker might follow to successfully infiltrate a network, gain unauthorized access to data, or perform some malicious act. The categories are also consistent with a model of attack detailed by Lockheed Martin called the Cyber Kill Chain.

Below the categorized display of alarm icons, USM Appliance displays a tabular listing of individual alarms, by default, in reverse chronological order. In addition, if you click on any of the blue circles, USM Appliance will display only the alarms corresponding to the selected circle. From the list of alarms, you can click on any individual alarm row to expand the display of information about the alarm. You can then click the **View Details** button, or click the  icon, to display more information on the selected alarm, including individual events that actually triggered the alarm.

The top section of the Alarms page display lets you search for and filter alarms that are displayed on the Alarms page. You can qualify alarms by event attributes such as sensor location, asset group, risk level, or OTX pulse.

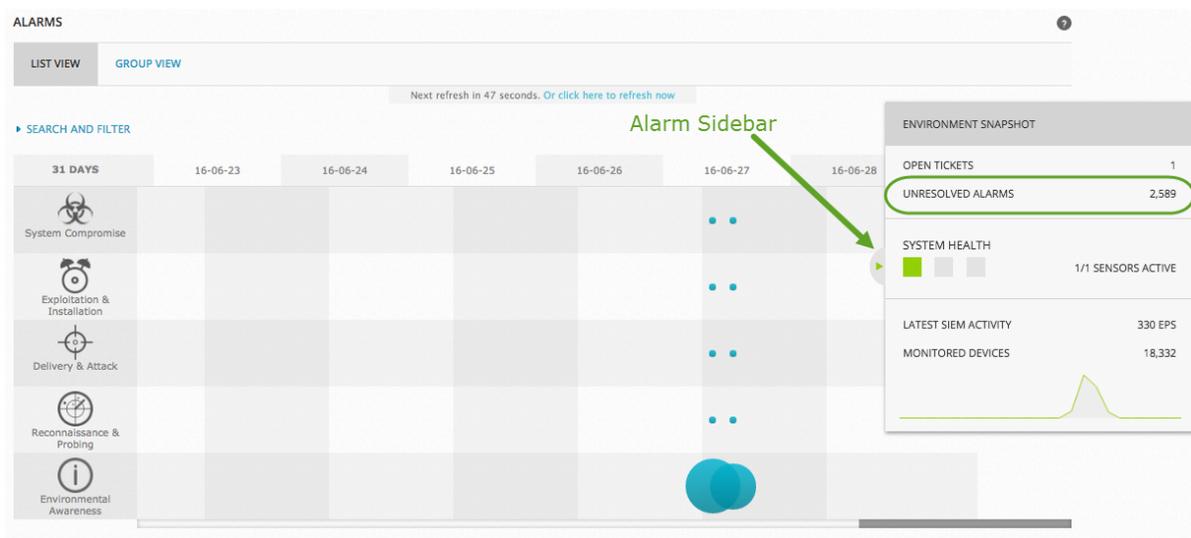
Reviewing Alarms as a Group

This task helps you sort alarms in bulk as a group when you have many alarms that are similar.

You can always switch to **List View** if you need more insight into specific alarms.

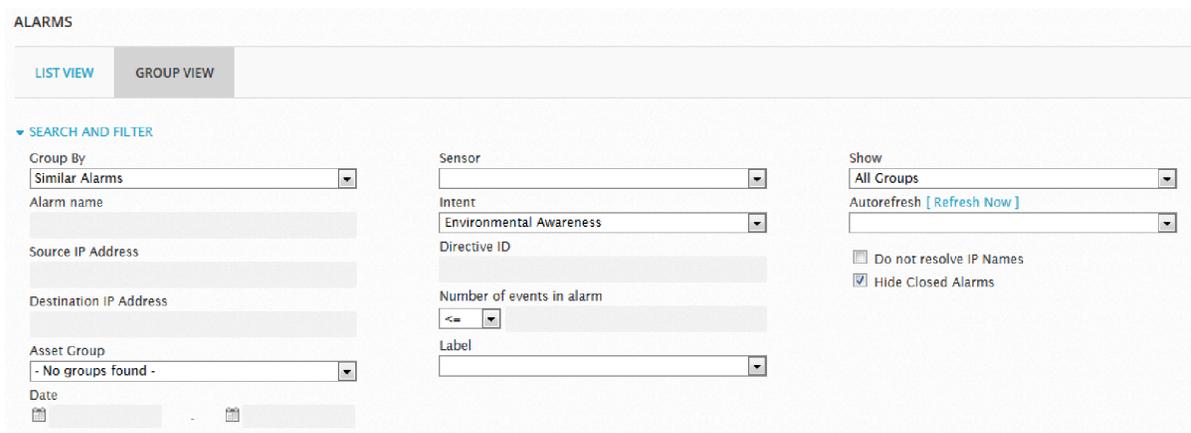
To review alarms in Group View

1. Go to **Analysis > Alarms**.
2. To see the number of unresolved alarms, click the Alarms page sidebar.



This sidebar shows the number of alarms reported in USM Appliance. A large number would normally only be present **before** you have created policies or customized correlation rules to exclude false positives. This may also show that you still need to update vulnerable software on certain, high-value assets.

3. To see how many similar alarms you have, select the **Group View** tab.



4. Under **Search and Filter**, select the criteria for the group, for example, alarms of the same category.

USM Appliance automatically displays all alarms corresponding to your filtering criteria.

You can also filter for alarms related to a specific USM Appliance sensor, a specific source or destination IP, and other useful filtering criteria.

5. Analyze the alarms, paying attention to the following in the order dictated by your incident plan:
 - Any alarms based on an Open Threat Exchange (OTX) pulse.
 - Any alarms with a source or destination IP, based on OTX IP Reputation data.
 - Alarms occurring with the greatest frequency. By analyzing and eliminating such events, whether harmful, relevant, or not, you reduce the number of events that USM Appliance or an analyst must process.
 - Examine new types of alarms. These indicate changes in network patterns and behavior.
 - Look at hosts that seem to be involved in a lot of alarms. This may indicate a vulnerable host or an infection of the host with malicious software.
 - Look at hosts that seem to be Identify the group of open alarms on which you want to take action.



Note: If an OTX pulse is creating too much noise and generating too many false positive alarms, you can unsubscribe from the pulse. In that case, you will still receive information about the threat in your pulse activity feed, but no raw data is pulled into USM Appliance for correlation and generation of alarms.

6. Identify any groups of alarms you want to investigate further, for example, any alarms with a higher risk than others in the group, such as **Delivery and Attack**.
7. Go to the **Alarms List View** and, for example, filter for the alarm intent.
8. After locating the alarm you want to investigate, take ownership of it. Taking ownership tells others on your team that you are actively investigating this, avoiding duplicate efforts.

Reviewing Alarms as a List

In most cases, the **List View** of the USM Appliance Alarms page provides you with the best starting place for analyzing alarms. (For field descriptions, see [Alarms list fields](#)).

You can review alarms in List View by one of two methods:

- Using the Alarm Graph to see where you have the most or the highest-risk alarms.
- Searching and filtering for alarms using specific criteria.

To review alarms as a list

1. Go to **Analysis > Alarms**.
2. On the far-right side of the Search and Filter section, toggle **Show Alarm Graph** to **Yes**.

The setting persists until you change it.

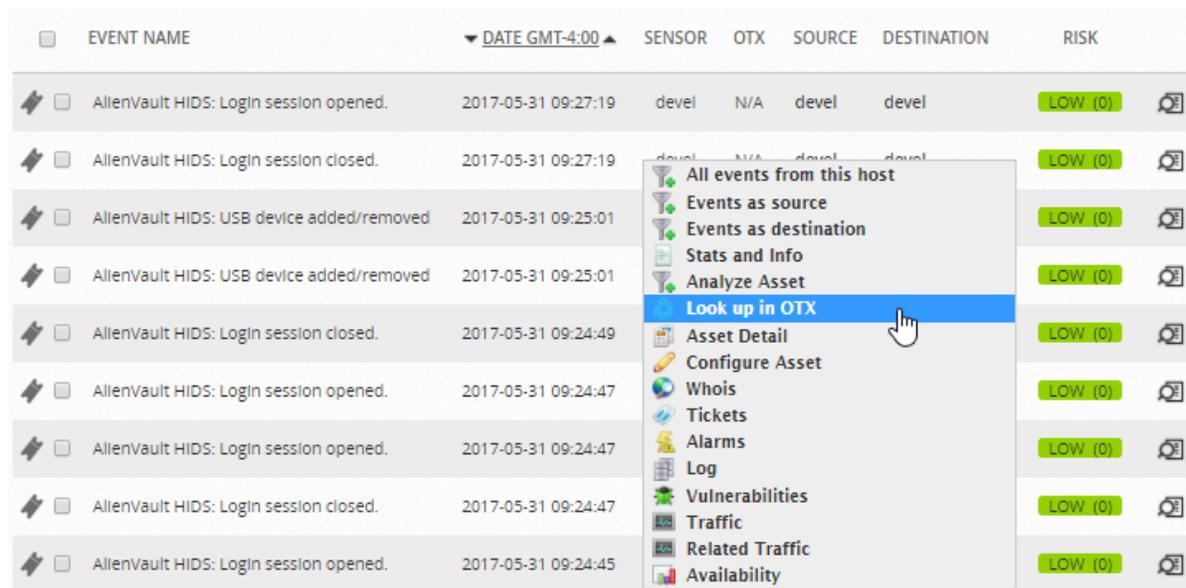
3. Review the **Alarm Graph** to assess the level and number of issues USM Appliance has found.

For details about how the Alarm Graph works, see [Filtering Alarms in List View](#).

4. Review the Alarms list, if necessary, using **Search and Filter** to get information about specific alarms.

For details about how Search and Filter works, see [Filtering Alarms in List View](#).

In addition to other navigation options, in both Alarm and SIEM Event list views, you can right-click on Source and Destination IP addresses or host names, which will display a popup menu of available actions you can take corresponding to a specific IP address or host name.



For example, the **Look up in OTX** option opens the OTX site to display potential and reported threats related to the selected location. If no threat information is found about the location, the **Look Up in OTX** option opens the Create New Pulse web page in OTX, which lets you create a new Pulse to report a possible new threat.

- Analyze the alarms, paying attention to the following, in the order dictated by your incident response plan:

- Alarms with the highest risk level.

These contain events with the highest reliability and priority, and involve assets with the highest value.

- Alarms occurring with the greatest frequency.

By analyzing and eliminating such events, whether harmful, relevant, or not, you reduce the number of events that USM Appliance or an analyst must process.

- Examine new types of alarms.

These indicate changes in network patterns and behavior. Look at hosts that seem to be involved in a lot of alarms. This may indicate a vulnerable host or an infection of the host with malicious software.

- Get more details about an alarm by clicking inside of its row in the list.

Note: If the alarm comes from an OTX pulse, clicking on the OTX icon takes you to OTX for research on the indicators comprising the pulse. If you want system details about the alarm, click anywhere else in the row. If you find that an OTX pulse is generating too many false positive alarms, you can always unsubscribe from the pulse .

The Alarms tray appears:

The screenshot shows the Alarms tray interface. At the top, there is a table with columns: DATE, STATUS, INTENT & STRATEGY, METHOD, RISK, OTX, SOURCE, and DESTINATION. Below the table, a detailed view for an alarm is shown. The alarm title is "ENVIRONMENTAL AWARENESS: DESKTOP SOFTWARE - CHAT CLIENT" with a subtitle "ATTACK PATTERN: EXTERNAL TO EXTERNAL ONE-TO-ONE". To the right of the title is a bar chart labeled "OPEN & CLOSED ALARMS". Further right are statistics: "TOTAL EVENTS 10" (with a date "2016-09-08 16:10:04"), "DURATION 2 HOURS", and "ELAPSED TIME 2 HOURS". On the far right, there are buttons for "VIEW DETAILS", "CLOSE", "DELETE", and "APPLY LABEL".

For field descriptions, see [Alarms Tray – Fields](#).

- Review the information to determine the reliability of the alarm.



Note: If the alarm contains only one event, it may not be as reliable as if it contained multiple events over a period of time. Only your detective work can find this out.

8. Get more details by clicking **View Details**. (For field descriptions, see [Alarm Details — Columns and Fields](#).)

a. Review the source and destination for this alarm.

Do these tell you anything environmentally?

b. Review the risk of this alarm. For details on risk calculation, see [USM Appliance Network Security Concepts and Terminology](#).

The screenshot shows the 'ALARMS' section in a web interface. It has tabs for 'LIST VIEW' and 'GROUP VIEW'. Below the tabs, there's a breadcrumb trail: 'Alarms > AV Policy violation, Google Talk IM usage on 10.216.76.117'. There's an 'ACTIONS' dropdown menu. The main content is a table with the following columns: Status, Risk, Attack Pattern, Created, Duration, # Events, Alarm ID, and OTX Indicators. The 'Risk' column is highlighted with a green box and shows 'LOW (1)'. Below the table, there are two sections for 'Source (1)' and 'Destination (1)', both highlighted with green boxes. The source IP is 10.216.76.117 and the destination IP is 74.125.206.125. Both have 'Asset Groups: Unknown', 'Networks: Unknown', and 'OTX IP Reputation: No'.

c. If you find an alarm you want to investigate further, see [Review Security Events](#).

9. If needed, go back to the Alarms list and use **Search and Filter** to get information about other alarms originating from a particular asset or of a certain type.

For details about how **Search and Filter** works, see [Filtering Alarms in List View](#).

Filtering Alarms in List View

Both a high-level overview and a detailed look at individual alarm types, the List View lets you filter alarms by one of two methods:

- Using the Alarm Graph to see where you have the most or the highest-risk alarms ([Filtering Alarms, Using the Alarm Graph](#)).
- Searching and filtering for alarms using specific criteria ([Using Specific Search and Filter Criteria for Alarms](#)).

Filtering Alarms, Using the Alarm Graph

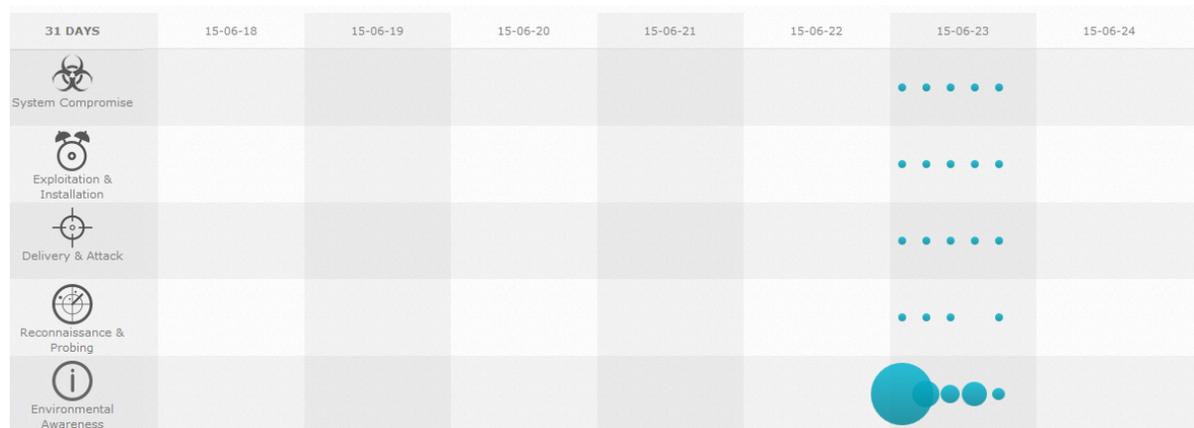
Alarms in the graph appear correlated by intent, based on the [Cyber Kill Chain model](#).

Blue bubbles of varying sizes indicate the relative number of alarms generated among your assets on each day within a 31-day period.

To expose the Alarm Graph

1. On the Alarms page, look for the label **Show Alarm Graph** on the far right of the Search and Filter section.
2. Click **No**.

This toggles the Alarm Graph to **Yes** and the Alarm Graph appears.



3. Hover over one of the bubbles to get more details.



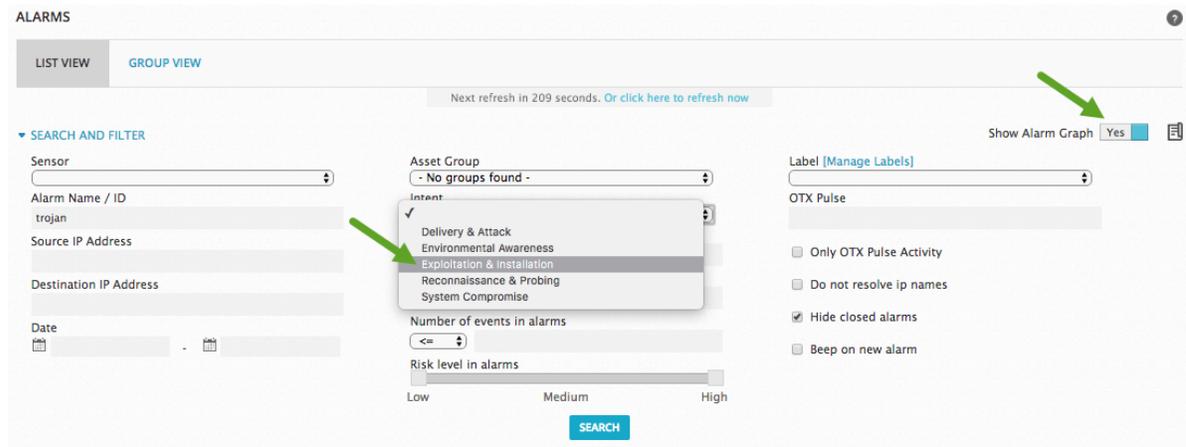
Each bubble represents the alarms of a specific intent for a three-hour period of one day in a 31-day cycle. Each exposes the following details:

- Time span in three-hour increments.
- Number of alarms.
- Top five strategies among these alarms, for example, spyware infection or worm infection.

4. Click one of the bubbles.

Now the Alarms list appearing below the graph shows just the alarms of the type and window of time you selected.

You can click on any of the alarms to see the event that triggered it. See [Review Security Events](#).



To hide the Alarm Graph from view

- Go to the **Show Alarm Graph** toggle (shown) and click the Yes default to toggle the setting to **No**.

The Alarm Graph now no longer displays.

- When you want to see it again, just toggle No to **Yes**.

Using Specific Search and Filter Criteria for Alarms

You can use the Search and Filter area of the Alarms page to search for specific alarms, based on the following criteria:

- Alarms from a specific USM Appliance Sensor
- Alarm name / ID
- Source and destination IP address
- Date range
- Asset Group
- Intent
- Directive ID
- Alarms containing certain event types
- Number of events in the alarm
- Risk level of the alarm
- Alarms exclusively from OTX pulses, or search on the pulse name.

Note: At this time, USM Appliance does not offer a filter for IP Reputation-based alarms. However, you can view these within the Alarms list, where they occur.

To filter for specific alarms

1. In the Search and Filter section of the Alarm page, select your search criteria and click **Search**.

Your search results appear in the Alarms List.

<input type="checkbox"/>	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION	<input type="checkbox"/>
<input type="checkbox"/>	13 hours		C&C Communication	Tinba DGA		N/A	10.218.99.10:1629	10.132.228.15:tcpnethasprv	
<input type="checkbox"/>	13 hours		Suspicious Behaviour	Suspicious user-agent detected		N/A	10.192.62.34:2955	205.167.7.126:password-chg	
<input type="checkbox"/>	13 hours		Adware infection	Generic		N/A	10.192.64.75:cadsi-lm	205.167.7.126:unitary	
<input type="checkbox"/>	13 hours		Suspicious Behaviour	Suspicious user-agent detected		N/A	10.132.3.79:2934	89.167.129.32:csnet-ns	
<input type="checkbox"/>	13 hours		Suspicious Behaviour	Suspicious user-agent detected		N/A	10.201.36.11:2429	205.167.7.126:234	
<input type="checkbox"/>	13 hours		Suspicious Behaviour	Suspicious user-agent detected		N/A	10.196.42.54:2387	205.167.7.126:gss-xlicen	
<input type="checkbox"/>	13 hours		Suspicious Behaviour	Suspicious user-agent detected		N/A	10.216.76.10:1657	81.52.140.11:micom-pfs	
<input type="checkbox"/>	2016-09-08 03:40:28	open	Worm infection	Internal Host scanning		N/A	10.149.32.27:2597	10.214.0.94:ftfp	

2. To see more details, click on one of the alarms ([Reviewing Alarms as a List](#)).

Note: **Hide closed alarms** is selected by default.

Alarms List — Fields

Alarms list fields

Column/Field Name	Description
Date	Date and time USM Appliance completed alarm correlation.
Status	Whether or not the alarm is open and still correlating, or closed.
Intent & Strategy	<p>Describes the attack pattern of indicators intruding on your system.</p> <p>Intent and strategy are based on the taxonomy, or classification, of a directive. For example, a directive of AV Malware might have an “intent” of system compromise, with a "strategy" of suspicious behavior. When alarms come from OTX pulses, the Intent is always Environmental Awareness and the Strategy is OTX Indicators of Compromise.</p> <div data-bbox="443 814 1421 1058" style="background-color: #e6f2ff; padding: 10px;"> <p> Note: Due to the size of the field label, only the strategy is visible from the Alarms list. However, when you click the row, thereby expanding the Alarms tray, the strategy becomes visible.</p> <p>The taxonomy for alarms with IP reputation data is based on the directive that generated the alarm.</p> </div>
Method	If known, the method of attack or infiltration associated with the indicator that generated the alarm. For OTX pulses, the method is the pulse name.
Risk	<p>Risk level of an alarm, which can be Low (1), Medium (2), or High (>=3) .</p> <p>Risk calculation is based on the formula: Asset Value * Event Reliability * Event Priority / 25 = Risk</p> <p>So if Asset Value = 3, Reliability = 4 and Priority = 5, the risk would be 3 * 4 * 5 / 25 = 2.4 (rounded down to 2), therefore the Risk value is Medium.</p>

Alarms list fields (Continued)

Column/Field Name	Description
OTX	<p>OTX icon present when events causing the alarm contained IP Reputation-related data or were from IoCs related to an OTX pulse.</p> <ul style="list-style-type: none"> • Orange — Alarm was generated by one of the following: <ul style="list-style-type: none"> ◦ A pulse ◦ Both IP Reputation and OTX pulse indicators. In this case, the pulse name displays. • Blue — Alarm contains IP Reputation data about one more of the IP address involved. • N/A — If no OTX data available.
Source	<p>Hostname or IP address of the source, with national flag if country is known, for an event creating the alarm.</p>
Destination	<p>Hostname or IP address of the destination, with national flag if country is known, that received the events generating the alarm.</p>

Alarms Tray – Fields

Alarms tray field descriptions USM Appliance

Field Name	Description
Intent & Strategy	<p>Describes the attack pattern of indicators intruding on your system.</p> <p>Intent and strategy are based on the taxonomy, or classification, of a directive. For example, a directive of AV Malware might have an “intent” of system compromise, with a strategy of suspicious behavior.</p> <p>When alarms come from OTX pulses, the Intent is always Environmental Awareness and the Strategy is OTX Indicators of Compromise.</p> <p>Note: Due to the size of the field label, only the strategy is visible from the Alarms list. However, when you click the row, thereby expanding the Alarms tray, the strategy becomes visible.</p> <p>The taxonomy for alarms with IP reputation data is based on the directive that generated the alarm.</p> <p>For more information, see Event Correlation.</p>
Open & Closed Alarms	<p>When you hover over the column heading, you see the date the alarms finished correlation; the number of open, correlating alarms; and the number of closed alarms.</p> <p>When green, the alarm is open and still correlating.</p>
Total Events	Number of events associated with an alarm.
Duration	Duration between the first event and the most recent event represented in this alarm.
Elapsed Time	Time since the first alarm was generated.

Alarm Details — Columns and Fields

Alarm Details field descriptions

Column/Field Name	Description
Status	Whether or not the alarm is open or was closed.
Risk	<p>Risk level of an alarm, which can be Low (1), Medium (2), or High (>=3) .</p> <p>Risk calculation is based on the formula: Asset Value * Event Reliability * Event Priority / 25 = Risk</p> <p>So if Asset Value = 3, Reliability = 4 and Priority = 5, the risk would be $3 * 4 * 5 / 25 = 2.4$ (rounded down to 2), therefore the Risk value is Medium.</p>
Attack Pattern	Analyzed method of infiltration or attack. Shows how the attack took place, for example, external to internal, one to many, external to external, or many to many.
Created	Date alarm was correlated
Duration	Duration between the first event and the most recent event creating the alarm.
# Events	Number of events associated with the alarm.
Alarm ID	Identification of the alarm.
OTX Indicators	Number of OTX pulse indicators, shown in blue, generating the alarm.
Source/Destination	Hostname or IP address of the host. The number in parentheses next to the label stands for the number of IPs or hosts involved with the events associated with this alarm.
<ul style="list-style-type: none"> Location 	If the country of origin is known, displays the national flag of the event responsible for the alarm.
<ul style="list-style-type: none"> Asset Groups 	<p>When the source/destination belongs to your asset inventory, displays any asset groups to which that asset belongs.</p> <p>When the source/destination is an external host, Assets Groups displays Unknown.</p> <p>When the source/destination is a host within one of your asset groups, these sections contain a value. You can click it to go to the Asset Details page for more information.</p>

Alarm Details field descriptions (Continued)

Column/Field Name	Description
<ul style="list-style-type: none"> • Networks 	<p>When the source/destination belongs to your asset inventory, displays any networks to which that asset belongs.</p> <p>When the source/destination originates from a host in an external network, Networks displays Unknown.</p> <p>When the source/destination of the alarm events comes from one of your networks, the field contains a value. You can click it to the Network Group Details page for more information.</p>
<ul style="list-style-type: none"> • OTX IP Reputation 	<p>(Yes/No) If “Yes,” the IP or hostname is known to IP Reputation and it may be malicious. It is, at minimum, suspicious.</p> <p>Note: When you click Yes, a popup displays, providing more information about the IP address. A hypertext link to the details about that IoC in OTX also appears, allowing you to better assess the threat.</p>
Open Ports	<p>Any open ports discovered by USM Appliance.</p> <p>If the source/destination is an asset in your inventory, displays all open ports detected.</p> <p>If the source/destination is an external host, displays any open ports detected, based on USM Appliance communication with that host.</p>
<ul style="list-style-type: none"> • Ports 	<p>You can select the number of ports you want to display in increments of 5, 10, and 20.</p>
<ul style="list-style-type: none"> • Port 	<p>Associated port number.</p>
<ul style="list-style-type: none"> • Service 	<p>Name of the service using the port, if applicable.</p>
Vulnerabilities, Properties, Notes	<p>These tabs appear only if the source/destination is an asset belonging to your asset inventory.</p>
<ul style="list-style-type: none"> • Vulnerabilities 	<p>Includes the service/port and severity of the vulnerability.</p>
<ul style="list-style-type: none"> • Properties 	<p>Lists all asset properties defined in Asset Details.</p>
<ul style="list-style-type: none"> • Notes 	<p>User-entered comments about the asset and/or alarm.</p>

Alarm Details field descriptions (Continued)

Column/Field Name	Description
Other Details	<p>Clicking SIEM Events and Raw Logs takes you to those respective pages, where filtering is based on the source/destination IP addresses. These pages provide information about other events or logs that reference the IP address for the alarm.</p> <p>Other links go to external security resources, such as Honey-Pot, Whois, or Reverse-DNS, where you may find out more about the particular IP.</p> <p>For information on these, see the <i>Open Threat Exchange (OTX) User Guide</i> or visit their respective websites.</p>
Events	<p>Lists the events that generated the alarm.</p> <p>Note: In general, whether events generate an alarm depends solely on the directive taxonomy in USM Appliance. However, IoC events from OTX pulses automatically generate an alarm.</p>
<ul style="list-style-type: none"> Alarm, Risk, Date, Source, Destination, OTX 	<p>For definitions, see above.</p>
<ul style="list-style-type: none"> Correlation level 	<p>Correlation level assigned, based on a rules hierarchy USM Appliance employs, with each rule assigned a priority and a reliability value.</p> <p>For details, see Event Correlation.</p>

Taking Ownership of an Alarm

As part of an alarm remediation response, you should take ownership of an alarm you want to work on. This tells others that you are actively investigating it. This avoids duplication of efforts.

To take ownership of an alarm

1. From **Analysis > Alarms > Group View**, locate an alarm you want to investigate.
2. Take ownership of the alarm by clicking **Take**, under the **Owner** column within its row.

The Owner status now changes from **Take** to **Release**, signifying that you now have responsibility for the alarm group.

3. Select the checkbox at the front of the alarm row.

The following two buttons now appear in the UI above the **Description**, **Status**, and **Action** columns:

- Close Selected
- Delete Selected



Note: Do not click either of these at this time.

The ticket icon under the **Action** column now also becomes active.

4. Under **Description**, type a *reason* for the action you want to take:
 - **Open a ticket** — Under **Action**, click the ticket icon to open a new ticket on the selected alarm group.

The **New Ticket** dialog box appears. See [Create a Ticket](#).
 - **Close or Delete an alarm** — Select the appropriate action; confirm it when prompted.
 - **Close** means an alarm still resides in the database. It does not, however, display in the web interface.
 - **Delete** means that you want to delete the alarm from the database.

You might close an alarm that you know is a false positive. An example of a false positive might be if instant messaging triggered an alarm, but your corporate security policy allows instant messaging. You should then create a policy to make sure that USM Appliance does not notify you about such events in the future. See [Tutorial: Create a Policy to Discard Events](#).

After that, you may want to delete all occurrences of this alarm from the SIEM.

The choice about whether to close or delete an alarm depends on your corporate compliance policy. If alarm retention is not a priority, you should delete them to save disk space.

Back Up and Restore Alarms

By default, USM Appliance stores alarms in the database until you delete them manually. To save disk space, AlienVault encourages that you delete alarms after they have been investigated or mediated, especially if the alarm is a false positive. You can also configure the alarms to expire after a certain time, then USM Appliance will purge the alarms automatically. The recommendation is to store alarms for 90 days for compliance and 30 days for data forensics.

Alarm Backup Configuration

To configure alarm expiration:

1. From the USM Appliance web interface, go to **Configuration > Administration > Main > Backup**.
2. Change **Alarms Expire** to **Yes**.

The Alarms Lifetime defaults to 0 (days), which means the alarms never expires.

3. Change **Alarms Lifetime** to a suitable number based on your environment and your company's requirement. For example, 90 days for compliance or 30 days for data forensics.

ADMINISTRATION

USERS MAIN BACKUPS

BACKUP ▲

Backup configuration: backup database, directory, interval

Enable SIEM database backup	Yes ▾	?
Number of Backup files to keep in the filesystem	30	?
Events to keep in the Database (Number of days)	90	?
Events to keep in the Database (Number of events)	40000000	?
Backup start time	01:00	?
Active Netflow Window	45	?
Alarms Expire	Yes ▾	?
Alarms Lifetime	7	?
Logger Expiration	No ▾	?
Active Logger Window	0	?
Password to encrypt backup files		?



Note: In new installations of USM Appliance version 5.8.6 or later, the default value for Alarms Expire is Yes and the default value for Alarms Lifetime is 90. This means that alarms older than 90 days are removed from the system.

4. Click **Update Configuration**.

After the alarms reach the Alarms Lifetime, USM Appliance removes them from the database every day and create a backup file in `/var/lib/ossim/backup_alarm`. The name of the file reads `alarm_restore_YYYY-mm-dd.sql.gz`.

Backing Up All the Alarms

To back up all the alarms on USM Appliance:

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.

The AlienVault Setup menu displays.

2. On the AlienVault Setup main menu, select **Jailbreak System** to gain command line access.

Select **Yes** when prompted. You will be in the root directory.

On the command line, type the following command:

```
screen
```

We recommend using the screen session so that you can keep the program running even after you log out.

- 3.
4. Stop the following services so that they do not interfere with the process:

```
/etc/init.d/monit stop
/etc/init.d/ossim-server stop
/etc/init.d/ossim-agent stop
/etc/init.d/ossim-framework stop
/etc/init.d/alienvault-api stop
```

5. Back up the alarms:

```
mysqldump -p`grep ^pass /etc/ossim/ossim_setup.conf | sed 's/pass=//'\` --
no-autocommit --single-transaction alienvault event extra_data idm_data
otx_data backlog_event backlog alarm component_tags tag alarm_ctxs alarm_
nets alarm_hosts | pigz > alienvault-alarms-`date +%s`.sql.gz
```

Adding ``date +%s`` to the filename gives it a unique time stamp.

This procedure creates the `alienvault-alarms-<timestamp>.sql.gz` file. Transfer the file to the target system. You can use either an SFTP client on Windows, such as WinSCP; or the SCP protocol on Linux.

Restoring Alarms

You can restore all the alarms using the output file generated from the procedure above (`alienvault-alarms-(timestamp).sql.gz`) or one of the daily backup files in `/var/lib/ossim/backup_alarm`.



Note: AlienVault recommends that you only restore the relevant alarms to avoid filling up the database.

Before following the procedure below, you should have deployed the SAME version of USM Appliance. You should have transferred the backup files to the target system and place them in the root directory.

To restore alarms

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.

The AlienVault Setup menu displays.

2. On the AlienVault Setup main menu, select **Jailbreak System** to gain command line access.

Select **Yes** when prompted. You will be in the root directory.

3. On the command line, type the following command:

```
screen
```

We recommend using the screen session so that you can keep the program running even after you log out.

4. Stop the following services so that they do not interfere with the process:

```
/etc/init.d/monit stop
/etc/init.d/ossim-server stop
/etc/init.d/ossim-agent stop
/etc/init.d/ossim-framework stop
/etc/init.d/alienvault-api stop
```

5. Restore the alarms:

```
zcat alienvault-alarms-<timestamp>.sql.gz | ossim-db
```

6. Restart all services for changes to apply:

```
alienvault-reconfig -c -v -d
```

Event Management

USM Appliance Server receives normalized log data called events from one or more USM Appliance Sensors, correlates and prioritizes them across all assets, and then present them in the web UI as a variety of summary and detailed views.

This section covers the following subtopics:

- [Events Page Overview](#) 143
- [USM Appliance Event Taxonomy](#) 144
- [Review Security Events](#) 149
- [Back Up and Restore Events](#) 169
- [Clear All Events from the SIEM Database](#) 173
- [Event Storage Best Practices](#) 174

Events Page Overview

When you select the **Analysis > Security Events (SIEM)** menu option, USM Appliance displays the following page.

The screenshot displays the Security Events (SIEM) interface. At the top, there are tabs for SIEM, REAL-TIME, and EXTERNAL DATABASES. Below this is a search bar with a 'GO' button. The main area contains several filter sections: SHOW EVENTS (Last Day, Last Week, Last Month, Date Range), DATA SOURCES, DATA SOURCE GROUPS, SENSORS, ASSET GROUPS, NETWORK GROUPS, RISK, OTX IP REPUTATION, and OTX PULSE. There is also an 'ADVANCED SEARCH' button. Below the filters, there are tabs for EVENTS, GROUPED, and TIMELINE, and a 'SHOW TREND GRAPH' toggle. The main content area shows a table of events with columns: EVENT NAME, DATE GMT-4:00, SENSOR, OTX, SOURCE, DESTINATION, and RISK. The table displays 7 events, all with a risk level of 'LOW (0)'. The total number of events in the database is 2,486,895.

EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:1200	10.192.98.57:7	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	208.100.40.44:2431	10.157.4.16:368	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	208.100.40.44:2525	10.196.42.34:503	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:2294	10.234.39.117:251	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.148.20:2294	10.201.68.97:297	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:2674	10.150.2.45:898	LOW (0)
AlienVault NIDS: "ETPRO POLICY Proxy.pac Download"	2016-09-19 18:57:29	devel	N/A	199.168.151.20:1232	10.192.78.13:766	LOW (0)

By default, the **Security Events (SIEM)** page displays a SIEM view of events. The USM Appliance web UI also provides two other options for displaying security events:

- **Real-Time**

View that shows events in progress in your network.

- **External Databases**

Display security events from an external AlienVault database that is associated with a different AlienVaultUSM Appliance installation. For more information on configuring a connection to an external AlienVault database, see [How to display Security Events from an External AlienVault Database](#).

From the SIEM option view, you can search and filter for events using time ranges and other event attribute criteria.

Below the Search Filter section of the page, USM Appliance provides a display of all events, or filtered events (if you specified search criteria for events). Any normalized log event, or any other event received or generated by any USM Appliance Sensor at the application, system, or network level will appear in the display unless a USM Appliance policy has filtered it out or you have specified search filter criteria.

From the tabular summary listing of events, you can click on a specific event row to view further details about that event in a popup window. You can also click the  icon in an event row to display event detail on a new page, which also lets you choose further actions to take with the current event.

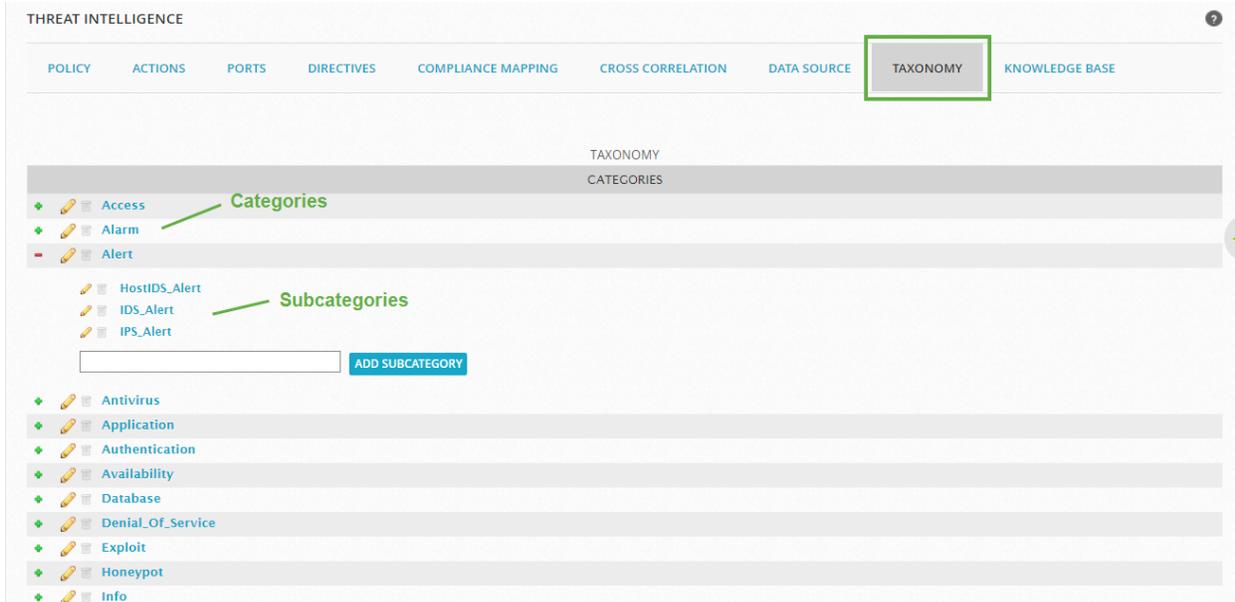
USM Appliance Event Taxonomy

AlienVault event taxonomy is a classification system for security events. It provides the USM Appliance correlation engine with a standardized framework of product types, categories, and subcategories on which to operate. Normalizing disparately formatted log entries received from different types of assets into taxonomy's single framework enables the correlation engine to detect patterns of behavior occurring across all managed assets.

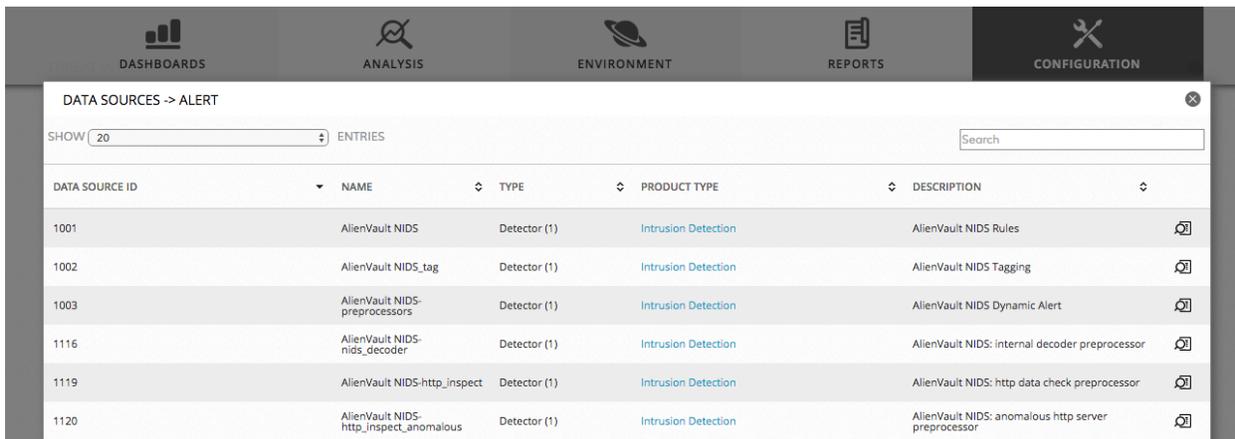
AlienVault event taxonomy is used in conjunction with data sources in the following areas on USM Appliance:

- **Policies** — Policy conditions use taxonomy to define the types of events that USM Appliance should process. Event types can be selected using either **DS Groups** or **Taxonomy**. See [Policy Conditions](#) for a description of taxonomy event types.
- **Correlation Directives** — Similar to policies, when creating a new directive, you can use taxonomy to specify the plugins (data sources) that the directive concentrates on.
- **Security Events** — Taxonomy information for individual security events is displayed on the event details page. See [Review Event Details](#) for more information.

To see a complete list of event taxonomy, go to **Configuration > Threat Intelligence > Taxonomy**. Click the green plus sign next to each category to display the subcategories.



Clicking the category or subcategory directly opens a new page displaying all the data sources associated with the category or subcategory respectively.



USM Appliance uses event taxonomy to classify data sources (the product type) and provide further granularity that defines the category and subcategory for each event type.

Go to **Configuration > Threat Intelligence > Data Source** to view the list of data sources and their product types.

THREAT INTELLIGENCE

POLICY ACTIONS PORTS DIRECTIVES COMPLIANCE MAPPING CROSS CORRELATION DATA SOURCE TAXONOMY KNOWLEDGE BASE

SHOW 20 ENTRIES

DATA SOURCE GROUPS

DATA SOURCE ID	NAME	TYPE	PRODUCT TYPE	DESCRIPTION
1517	ntsyslog	Detector (1)	Operating System	Windows NT/2000/XP syslog service
1518	mswindows	Detector (1)	Operating System	MS Windows Events
1519	netgear	Detector (1)	Firewall	Netgear
1520	netscreen-manager	Detector (1)	Management Platform	Juniper Netscreen Security Manager
1521	postfix	Detector (1)	Mail Server	Postfix mailer
1522	netscreen-firewall	Detector (1)	Firewall	Juniper Netscreen Firewall

Click the  icon to view the category and subcategories assigned to the event type:

THREAT INTELLIGENCE

POLICY ACTIONS PORTS DIRECTIVES COMPLIANCE MAPPING CROSS CORRELATION DATA SOURCE TAXONOMY KNOWLEDGE BASE

INSERT NEW EVENT TYPE

SHOW 20 ENTRIES

DATA SOURCE ID	EVENT TYPE ID	CATEGORY	SUBCATEGORY	CLASS	NAME	PRIORITY	RELIABILITY
1517	1	Database	Misc	-	ntsyslog: \Device\ACPIEC: The embedded controller (EC) hardware didn't respond within the timeout period.	1	1
1517	2	Database	Misc	-	ntsyslog: The 3ware Escalade Service should be removed ((number))	1	1
1517	3	Database	Misc	-	ntsyslog: \Device\ACPIEC: The embedded controller (EC) hardware returned data when none was requested.	1	1

Product Types and Categories

AlienVault event taxonomy consists of product types, categories, and subcategories.

USM Appliance Event Taxonomy — Product Types

Product Types		
• Alarm	• Honeypot	• Other Devices
• AlienVault Devices	• Infrastructure Monitoring	• Proxy
• Anomaly Detection	• Intrusion Detection	• Remote Application Access

USM Appliance Event Taxonomy — Product Types (Continued)

Product Types		
• Antivirus	• Intrusion Prevention	• Router/Switch
• Application	• Load Balancer	• Server
• Application Firewall	• Mail Security	• Unified threat management
• Authentication and DHCP	• Mail Server	• VPN
• Data Protection	• Management Platform	• Vulnerability Scanner
• Database	• Network Access Control	• Web Server
• Endpoint Security	• Network Discovery	• Wireless Security/Managemet
• Firewall	• Operating System	

Available options for categories will differ depending on which product type you select, and available options for subcategories will differ depending on which category you select.

USM Appliance Event Taxonomy — Categories

Category	Category Description
Access	An event that indicates a particular system, service, or resource is being used.
Alarm	
Alert	An alarm triggered from a security detection system.
Analysis	
Anomalies	
Antivirus	An event from an antivirus (or other endpoint security control) system.
Application	A log entry from an application or service that cannot be matched to one of the other categories in the USM Appliance taxonomy.
Authentication	An event from an authentication system, or the authentication sub-component of an application or operating system.
Availability	An event from a resource-availability monitoring system.
Correlation	

USM Appliance Event Taxonomy — Categories (Continued)

Category	Category Description
Correlation_Directives	
Cross_Correlation_Rules	
Database	
Hashboards	
Denial_Of_Service	A possible denial-of-service attack has been detected via correlating events seen on the network.
Exploit	Indicates the possible exploitation of a known vulnerability in a particular application or operating system.
Honeypot	This is an event from a honeypot system. Any connection to them is assumed to be either from a mis-configured system or a malicious source.
Incidents	
Info	An informational event, usually without direct significance to security. General system logs often fall into this category.
Inventory	An event from an inventory management system, probably the systems built into USM Appliance.
Knowledge_DB	
Malware	Malware has been detected, either running on a system, being transferred over the network, or communicating with a command-and-control system.
Monitor	
Network	
Policy	A violation of your company's usage policy has been detected.. This may be in the form of unapproved software installations, Internet services, or security configurations.
Policy_and_Actions	
Recon	A system has been detected scanning other systems on the network.

USM Appliance Event Taxonomy — Categories (Continued)

Category	Category Description
Reports	
SEIM_ Components	
SEIM_ Components_ Databases	
SEIM_ Components_ Servers	
Suspicious	This event represents a log entry that is unusual within the context of the system it originates from.
System	
Tools	
Voip	This is an event from a Voice-Over-IP communication system.
Vulnerabilities	
Wireless	This is an event from a wireless Ethernet (802.11) device.

Review Security Events

When investigating alarms, you may find it helpful to check whether there are any related events in the SIEM database that were not included in the alarm. For example, you could search for events that came from the same host as offending traffic triggering an alarm.

Most of the time, however, you can do one of the following to view events:

- From the **Analysis > Alarms**, access events that triggered the alarm by clicking the alarm in the **Alarms list > View Details** and clicking any related event in the **Events** list, located at the bottom of Alarm Details.
- From **Analysis > Security Events (SIEM) > SIEM**, search on events with specific criteria in mind, such as source and destination, a particular sensor or other relevant asset. See [Security Events Views](#) for details.

USM Appliance, complements the collection of regular security events and alarms with anomaly events. USM Appliance uses the log information collected from Identity Management (IDM) plugins and agent software to track the value of specific host attributes and generate anomaly-type events when those values change.

Examine Alarms and Security Events

In this procedure, we describe the first and most straightforward method of investigating the trigger for a specific alarm.

To get information on events that triggered an alarm

1. Go to **Analysis > Alarms** and click the alarm within the Alarms list whose events you want to research.

This could be based on the Alarm intent or some other factor.

2. Click **View Details**.
3. On Alarm Details in the **Events** list at the bottom of the page, click one of the related events.

The Event Details view displays.

This view provides as many details as USM Appliance knows about the event, including its risk, reliability and priority.

Depending on the event, the Event Details may include

- An attack payload description.
 - Rule detection details if a particular correlation rule flagged the event.
 - A concise view of the **Raw Log**.
4. To see more details, click **View More**.
 5. Examine information on the event ([Review Event Details](#)). For example, find out more about an involved source or destination IP address by clicking the respective IPs in the **Source** or **Destination** sections of the page.
 6. If one of your assets was involved with an alarm, get more information by going to **Environment > Assets & Groups > Assets ()**.
 - If the alarm is based on an attack, verify whether or not it really affects your asset.
 - Check the asset operating system and the services running on it. (This check requires you to learn what kinds of endpoints the attack targeted.)

- When examining assets, give special attention to any issues the vulnerability scan detected. If you see many vulnerabilities in an asset, examine them to determine the severity of each ([Viewing the Scan Results](#)).
7. Examine all reported alarms and events involving this asset to rule out any activity related to the alarm.

Based on the policies you configure, for example, about how USM Appliance should handle events from other tools, some events may not be stored in the SIEM database. However, the risk assessment engine still correlates them and assesses risk to create alarms.

8. To locate these and to check for any patterns of questionable asset activity, review the Raw Log.

Filter and Display Anomaly Events

The USM Appliance Server displays anomaly events, along with any other security events it processes, in the USM Appliance web UI's Security Events (SIEM) display.

To filter and display anomaly events

1. Select **Analysis > System Events (SIEM)** from the USM Appliance web UI.
2. In the top Search/Filter portion of the display, select the **Anomalies** option in the **Data Sources** field.



Note: The **Anomalies** option will only appear if the USM Appliance Server has anomaly events to display.

The USM Appliance web UI now displays the anomaly events generated by the USM Appliance Server within the specified time frame, and meeting any other filter conditions you specified.

SECURITY EVENTS (SIEM)

SIEM REAL-TIME EXTERNAL DATABASES

Search Event Name GO

SHOW EVENTS

- Last Day
- Last Week
- Last Month
- Date Range

DATA SOURCES: Anomalies

DATA SOURCE GROUPS:

SENSORS: EXCLUDE

ASSET GROUPS:

NETWORK GROUPS:

RISK:

OTX IP REPUTATION:

OTX PULSE:

ONLY OTX PULSE ACTIVITY

userdata1 like

anomalies x Last Day x

ADVANCED SEARCH

EVENTS GROUPED TIMELINE

SHOW ENTRIES

SHOW TREND GRAPH Off

DISPLAYING 1 TO 50 OF HUNDREDS OF EVENTS. 3,117 TOTAL EVENTS IN DATABASE.

<input type="checkbox"/>	EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK	
<input type="checkbox"/>	Machine state change	2017-06-21 07:57:46	VirtualUSMAllInOne	N/A	Host-192-168-183-130	Host-192-168-183-130	LOW (0)	
<input type="checkbox"/>	Host operating system change	2017-06-21 07:57:46	VirtualUSMAllInOne	N/A	manolito.pepito@WORKGROUP	manolito.pepito@WORKGROUP	LOW (0)	
<input type="checkbox"/>	Machine state change	2017-06-21 07:57:46	VirtualUSMAllInOne	N/A	manolito.pepito@WORKGROUP	manolito.pepito@WORKGROUP	LOW (0)	
<input type="checkbox"/>	Host operating system change	2017-06-21 07:57:46	VirtualUSMAllInOne	N/A	ivan	ivan	LOW (0)	
<input type="checkbox"/>	Host operating system change	2017-06-21 07:57:46	VirtualUSMAllInOne	N/A	Host-192-168-217-157	Host-192-168-217-157	LOW (0)	

- To view details of a specific anomaly, click the **Event Detail**  icon located on the far right of an event row.

The USM Appliance web UI now displays details of the selected event.

DATE	2017-02-03 10:51:33 GMT-5:00	CATEGORY	System
ALIENVAULT SENSOR	AllInOne [10.101.1.25]	SUB-CATEGORY	Information
DEVICE IP	N/A	DATA SOURCE NAME	anomalies
EVENT TYPE ID	1	DATA SOURCE ID	5004
UNIQUE EVENT ID#	9079255e-ea28-11e6-8abc-0025a2ee55b4	PRODUCT TYPE	Anomaly Detection
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
1	1	LOW (0)	0

SOURCE occomm2 [10.101.0.191]		DESTINATION occomm2 [10.101.0.191]	
Hostname: occomm2	Location: N/A	Hostname: occomm2	Location: N/A
MAC Address: 84:3A:4B:94:CC:50	Context: N/A	MAC Address: 84:3A:4B:94:CC:50	Context: N/A
Port: 0	Asset Groups: N/A	Port: 0	Asset Groups: N/A
Latest update: N/A	Networks: Pvt_010, ORDA_OC-10.101.0.x-23	Latest update: N/A	Networks: Pvt_010, ORDA_OC-10.101.0.x-23
Username & Domain: N/A	Logged Users: N/A	Username & Domain: N/A	Logged Users: N/A
Asset Value: 2	OTX IP Reputation: No	Asset Value: 2	OTX IP Reputation: No

LAST VALUE	NEW VALUE
Microsoft Windows RPC (unknown/tcp49153)	Microsoft Windows RPC (msrpc/tcp49153)

- The anomaly event detail identifies the Anomalies Data Source Name and Data Source ID (5004). Near the bottom of the event detail display, the Last Value and New Value entries highlight the change in IDM properties that triggered the generation of the anomaly event.

To display anomaly event types

You can identify the different types of events that the USM Appliance Server will generate for changes in IDM properties by viewing the details of the Anomalies data source configuration. To do that:

- Select **Configuration > Threat Intelligence** from the USM Appliance web UI.
- Select the **Data Source** option from the main Threat Intelligence display.

The USM Appliance web UI now displays a list of all data sources or plugins that are available.

- In the Search field, type "**anomalies**" or "**5004**" (the Anomaly data source ID).

The USM Appliance web UI now displays only a single row description of the Anomalies data source.

THREAT INTELLIGENCE

POLICY ACTIONS PORTS DIRECTIVES COMPLIANCE MAPPING CROSS CORRELATION **DATA SOURCE** TAXONOMY KNOWLEDGE BASE

SHOW [20] ENTRIES DATA SOURCE GROUPS [5004]

DATA SOURCE ID	NAME	TYPE	PRODUCT TYPE	DESCRIPTION
5004	anomalies	Detector (1)	Anomaly Detection	Inventory anomalies

SHOWING 1 TO 1 OF 1 PLUGINS FIRST PREVIOUS 1 NEXT LAST

4. Click the **Data Source Detail**  icon.

The USM Appliance web UI now displays all the individual event types the USM Appliance Server will generate for changes detected by enabled IDM plugins.

THREAT INTELLIGENCE

POLICY ACTIONS PORTS DIRECTIVES COMPLIANCE MAPPING CROSS CORRELATION **DATA SOURCE** TAXONOMY KNOWLEDGE BASE

SHOW [20] ENTRIES INSERT NEW EVENT TYPE

Search

DATA SOURCE ID	EVENT TYPE ID	CATEGORY	SUBCATEGORY	CLASS	NAME	PRIORITY	RELIABILITY	
5004	1	System	Information	-	Host service change	1	1	
5004	2	System	Information	-	Host operating system change	1	1	
5004	3	System	Information	-	IP address change	1	1	
5004	4	System	Information	-	Hostname change	1	1	
5004	5	System	Information	-	Machine state change	1	1	
5004	6	System	Information	-	CPU state change	1	1	
5004	7	System	Information	-	RAM memory state change	1	1	
5004	8	System	Information	-	Graphic card state change	1	1	

SHOWING 1 TO 8 OF 8 EVENT TYPES FIRST PREVIOUS 1 NEXT LAST

5. From this display you can set specific priority and reliability values for each type of event. You can also click the **Event Type Detail**  icon to change event type attributes, including the text description of the event type, and its configurable priority and reliability values.

Security Events Views

The Security Events (SIEM) page, under **Analysis > Security Events (SIEM)**, consists of two views: **SIEM View** and **Real-Time View**. You can also create your own **Custom Views** with specific search criteria and column selections.

SIEM View

This view offers search and robust filtering categories for isolating types of events to review.

From the tabular summary listing of events, you can click on a specific event row to view further details about that event in a popup window. You can also click the **More Details**  icon in an event row to display event details on a new page, which also lets you choose further actions to take with the current event. For field references, see [Review Event Details](#)

The Search Field

Enter the keyword of the event and click **GO** to start the search. By default, USM Appliance searches the Event Name, but you can change it by using the drop-down menu. Other field include

- Event ID
- Payload
- IDM Username
- IDM Hostname
- IDM Domain
- Src or Dst IP
- Src IP
- Dst IP
- Src or Dst Host
- Src Host
- Dst Host

You can use logical operators such as AND, OR, or ! (negation) to form a complex search. For Advanced Search options, see [Define Advanced Search Criteria for Security Events \(SIEM\)](#).

SIEM Event Filters

Using the filtering categories at the top of the Security Events (SIEM) page, you can search for specific events. For example,

- Events having the same host as the traffic that triggered an alarm.
- Events coming through the same sensor.
- Events based on OTX pulses or on OTX IP Reputation.

When you use multiple filters, USM Appliance sees the relationship between them as *AND*. Although you can make a selection from multiple filter groups to search on, you cannot select multiples from the same filter group. You can clear any or all existing filters at far-right.

Event filters

Filter Name	Description
Show Events	Date oriented filters, including a range filter, so that you can search events occurring within a specific time period.
Userdata list	Allows you to select from userdata1~userdata9, filename, username, or password to create a search criterion. Select the operator you want to use and enter the keyword in the field.
Data Sources	External applications whose data are collected and evaluated by a plugin, and translated into an event within the USM Appliance taxonomy.
Data Source Groups	A predefined list of usually related data sources, such as directive events.
Sensors	USM Appliance Sensor that captured the event. Select "Exclude" if you want to exclude events from this sensor instead.
Asset Groups	List of predefined asset groups.
Network Groups	List of predefined network groups.
Risk	<p>Risk level of the event, which can be Low (0), Medium (1), or High (>= 2).</p> <p>Risk calculation is based on the formula: $\text{Asset Value} * \text{Event Reliability} * \text{Event Priority} / 25 = \text{Risk}$.</p> <p>if Asset Value = 3, Reliability = 2 and Priority = 2, the risk would be $3 * 2 * 2 / 25 = 0.48$ (rounded down to 0). Risk is Low.</p>
OTX IP Reputation	<p>Clicking the list icon expands the list to show a set of IP Reputation filters.</p> <p>These let you see all events with IP Reputation data or, alternatively, only events with IP Reputation data of a specified severity level, or type of malicious activity.</p> <p>IP Reputation ranks severity based on the number of reports existing about an IP address, as well as the nature of the threat the IP poses.</p>

Event filters (Continued)

Filter Name	Description
OTX Pulse	<p>Double-clicking this field expands a list of pulse names, from which you then select a pulse to review as an event.</p> <p>If you know the pulse name, you can type it within the field. This quickly displays the pulse from the list.</p>
Only OTX Pulse Activity	<p>Shows all events within your environment resulting solely from OTX pulse indicators.</p> <p>Note: You cannot filter on events with IP Reputation data and OTX pulses simultaneously.</p>

SIEM Events List

The events themselves appear in a list in the second half of the view.

EVENTS		GROUPED	TIMELINE			CHANGE VIEW	ACTIONS
SHOW TREND GRAPH		Off				14,849,614 TOTAL EVENTS IN DATABASE.	
DISPLAYING 1 TO 50 OF MILLIONS OF EVENTS.							
<input type="checkbox"/>	EVENT NAME	▼ DATE GMT-4:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	RISK
<input type="checkbox"/>	directive_event: AV Policy violation, important host using Apple iTunes application detected on 10.143.8.37	2016-09-08 16:35:39	N/A	N/A	10.143.8.37:2755	205.167.7.126:618	LOW (0)
<input type="checkbox"/>	directive_event: AV Policy violation, vulnerable java version detected on 10.157.22.222	2016-09-08 16:35:38	N/A	N/A	10.157.22.222:2353	195.87.150.104:247	MED. (1)
<input type="checkbox"/>	directive_event: AV Policy violation, vulnerable Adobe Flash detected on 10.210.46.152	2016-09-08 16:35:36	N/A	N/A	10.210.46.152:2094	41.160.184.26:835	MED. (1)
<input type="checkbox"/>	directive_event: AV Policy violation, password in cleartext detected in HTTP traffic on 10.149.32.27	2016-09-08 16:35:36	N/A	N/A	10.214.26.221:1905	10.149.32.27:55	MED. (1)
<input type="checkbox"/>	directive_event: AV Bruteforce attack, SSH authentication attack against 10.157.7.4	2016-09-08 16:35:18	N/A	N/A	139.158.161.108:2561	10.157.7.4:848	MED. (1)

SIEM Events list columns in the Default view

Column Name	Description
Event Name	Name of the event.
Date	Date and time registered by USM Appliance for the event. Date and time are user configured.
Sensor	Name of USM Appliance Sensor detecting the event.
OTX	<ul style="list-style-type: none"> Orange — Alarm was generated either by an OTX pulse Blue — Alarm contains IP Reputation data about one more of the IP address involved.

SIEM Events list columns in the Default view (Continued)

Column Name	Description
Source	Hostname or IP address of the host, with national flag if country is known, that initiates the event.
Destination	Hostname or IP address of the host, with national flag if country is known, that receives the event.
Risk	<p>Risk level of the event, which can be Low (0), Medium (1), or High (≥ 2).</p> <p>Risk calculation is based on the formula: $\text{Asset Value} * \text{Event Reliability} * \text{Event Priority} / 25 = \text{Risk}$.</p> <p>if Asset Value = 3, Reliability = 2 and Priority = 2, the risk would be $3 * 2 * 2 / 25 = 0.48$ (rounded down to 0). Risk is Low.</p>
Magnifying glass icon 	<p>Clicking the magnifying glass takes you to the Event Details. (See Review Event Details.)</p> <p>Note: You can go to Event Details by clicking anywhere within the event, with the exception of the OTX icon.</p>

In addition to other navigation options, in both Alarm and SIEM Event list views, you can right-click on Source and Destination IP addresses or host names, which will display a popup menu of available actions you can take corresponding to a specific IP address or host name.

<input type="checkbox"/>	EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK	
	AllenVault HIDS: Login session opened.	2017-05-31 09:27:19	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: Login session closed.	2017-05-31 09:27:19	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: USB device added/removed	2017-05-31 09:25:01	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: USB device added/removed	2017-05-31 09:25:01	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: Login session closed.	2017-05-31 09:24:49	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: Login session opened.	2017-05-31 09:24:47	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: Login session opened.	2017-05-31 09:24:47	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: Login session closed.	2017-05-31 09:24:47	devel	N/A	devel	devel	LOW (0)	
	AllenVault HIDS: Login session opened.	2017-05-31 09:24:45	devel	N/A	devel	devel	LOW (0)	

-  All events from this host
-  Events as source
-  Events as destination
-  Stats and Info
-  Analyze Asset
-  Look up in OTX
-  Asset Detail
-  Configure Asset
-  Whois
-  Tickets
-  Alarms
-  Log
-  Vulnerabilities
-  Traffic
- Related Traffic
- Availability

For example, the **Look up in OTX** option opens the OTX site to display potential and reported threats related to the selected location. If no threat information is found about the location, the **Look Up in OTX** option opens the Create New Pulse web page in OTX, which lets you create a new Pulse to report a possible new threat.

Real-Time View

The Real-Time view shows you an up-to-the-minute snapshot of all events occurring within your system.

This view may or may not contain any OTX data, depending on what events are currently transpiring in your system.

Real-Time Events List

Real-Time view displays the Events list at the top of the page. The Events list in Real-Time view displays many of the same categories of information as SIEM view, but with some differences, and also unique information.

Real-Time Event Filters

Filters correspond to the hosts displayed.

To expand a filter list

- Left-click or start typing inside of the field.

This expands a list of filters for you to select from:

2016-01-11 17:32:59	directive_event: AV Policy violation, vulnerable Adobe Flash detected on SRC_IP	1	directive_alert	N/A	N/A	10.137.181.35:1566
2016-01-11 17:32:56	directive_event: AV Policy violation, vulnerable Adobe Flash detected on SRC_IP	1	directive_alert	N/A	N/A	10.157.22.64:1870

FILTERS

<p>Source IP: <input type="text" value="1"/> 🗑️</p> <p>Source Port: <input type="text" value="1"/> 🗑️</p> <p>Protocol: <input type="text" value="1"/> 🗑️</p> <p>Plugins: Show Plugin f</p> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> <ul style="list-style-type: none"> <li style="background-color: #e0f0ff; padding: 2px;">Host-192-168-254-6 [Host:192.168.254.6] <li style="padding: 2px;">Host-192-168-170-11 [Host:192.168.170.11] <li style="padding: 2px;">Host-192-168-118-185 [Host:192.168.118.185] <li style="padding: 2px;">Host-192-168-248-180 [Host:192.168.248.180] </div>	<p>Destination IP: <input type="text"/> 🗑️</p> <p>Destination Port: <input type="text"/> 🗑️</p> <p>Include OTX Info: <input checked="" type="checkbox"/></p>
---	--

If you already know the individual filter

- Type the filter identifier into the field.

The display jumps to that entry in the list.

- If USM Appliance finds real-time events for the filter you select, they display in the Events list.
- If USM Appliance does not find real-time events for that filter, the Events list appears empty.

To filter on plug-ins

- Click the **Show Plugin filter**.

A list of all supported system plugins displays at the bottom of the page. Not all of these are necessarily installed on your system. You must verify which plugins match your USM Appliance deployment.

Custom Views

When examining the Events list, USM Appliance allows you to edit the default views or create custom views with your specific search criteria and column selections.

To create a custom view for events

1. Go to **Analysis > Security Events (SIEM)** and perform a search to include the events you want to see.
2. Click **Change View** to select a predefined view.

Predefined views include Default, Taxonomy, Reputation, Detail, Risk Analysis, and IDM. Each view displays the same events but with different columns.

3. Alternatively, click **Change View** and then select **Create New View**.
 - a. In Create New Custom View, select the columns you want to see in this view.
 - b. To apply the same query every time when you launch this view, select **Include custom search criteria in this predefined view**.
 - c. Type a name for the view, and then click **Create**.

USM Appliance saves your changes and refreshes the page to display the view.

To delete a custom view for events

1. On **Analysis > Security Events (SIEM)**, click **Change View** to select the view you want to delete.
2. Click **Change View** again and select **Edit Current View**.
3. In Edit Current View, click **Delete** at the bottom.
4. Confirm the action when prompted.

USM Appliance deletes the corresponding view and refreshes the page to display the Default view.

Define Advanced Search Criteria for Security Events (SIEM)

This topic describes how to define advanced search criteria when performing a search on **Analysis > Security Events (SIEM)**.

When you click **Advanced Search**, the following window opens:

ADVANCED SEARCH

SENSOR: { any Sensor } ▾

__ ▾ >= ▾ Oct ▾ 07 2019 ▾ 23 : □ : □ __ ▾

EVENT TIME: AND ▾

__ ▾ { time } ▾ { month } ▾ □ { year } ▾ □ : □ : □ __ ▾

PRIORITY: RISK: { any risk } ▾ PRIORITY: == ▾ { any Priority } ▾

ASSET: == ▾ { any Asset } ▾ RELIABILITY: == ▾ { any Reliability } ▾

▶ IP FILTER

▶ PAYLOAD FILTER

▶ EVENT TAXONOMY FILTER

QUERY DB

This new window allows for detailed search on Event Time, Priority, IP, Payload, or Event Taxonomy. Click **Query DB** to start the search after you have specified the criteria.

Sensor

This filter allows you to select a deployed USM Appliance Sensor from the list.

Event Time

This option allows for fine grain filtering for events that occurred at a specific date and time.

Use the "time" drop-down to select greater than (>), less than (<), or not equal (!=) operators. You can use a wildcard (*) when specifying the time of the event. Select the "AND" or "OR" operator if you need to limit the search within two time settings.

Example:

In the screenshot below, the selections made will search for events that occurred after (>=) 10:00:00 AND before (<=) 11:00:00 on the 12th of July 2018, reducing the time frame to one particular hour on one specific date.

EVENT TIME:

>= Jul 12 2018 10 : 00 : 00

AND

<= Jul 12 2018 11 : 00 : 00

Priority

This filter allows you to specify the Asset Value , Event Reliability and Event Priority individually.

Example:

In the screenshot below, the options specified will search for events with an Asset value of 2, a Reliability greater than 4, and a Priority of 3 or more.

PRIORITY :

ASSET : = 2

RELIABILITY : > 4

IP Filter

Click **IP Filter** to display the options, which allow you to specify Layer 3 IP addresses and Layer 4 TCP or UDP protocols.

▼ IP FILTER

ADDRESS: { address } = **ADD M**

LAYER-4: **TCP** **UDP**

Click **Add More** to specify additional IP addresses. You can select "AND" or "OR" to combine them:

ADDRESS: Source = **OR** Dest = **ADD MO**

If you want to add a port number for TCP or UDP, click the corresponding button to display the options. For example

▼ IP FILTER:

ADDRESS : Source =

LAYER-4 : **NO LAYER4** **UDP**

TCP FILTER : source port =

Click **Add More** to specify additional port numbers. You can select "AND" or "OR" to combine them.

Payload Filter

Click **Payload Filter** to display the options, which allow you to specify what you want to search in the payload of an event.

▼ PAYLOAD FILTER

INPUT CRITERIA ENCODING TYPE: { encoding } ▾ CONVERT TO (WHEN SEARCHING): {

▾ { payload } ▾

Using the **encoding** and **Convert To** drop-down, you can convert the search string from ASCII to HEX, for example, should it be required.

Click **Add More** to specify additional payload criteria. You can select "AND" or "OR" to combine them.

Example:

The example below specifies criteria to search for events that contain the string "testmyids.com" OR "google.com" in the payload:

▼ PAYLOAD FILTER

INPUT CRITERIA ENCODING TYPE: { encoding } ▾ CONVERT TO (WHEN SEARCHING): {

(▾ has ▾ testmyids.com

▾ has ▾ google.com

 **Important:** Do not include quotes when entering the search strings.

Event Taxonomy Filter

Event Taxonomy Filter allows you to search for events using event taxonomy.

▼ EVENT TAXONOMY FILTER

PRODUCT TYPE:

EVENT CATEGORY:

For details on product type and event category, see [Product Types and Categories](#).

Review Event Details

Event Details identifies all information USM Appliance collected about this event. It also displays the number of indicators involved, when the event relates to an Open Threat Exchange® (OTX™) pulse, and the IP reputation-calculated reliability and risk level data.

AlienVault HIDS: Login session closed.

DATE	2018-04-04 15:07:58 GMT-4:00	CATEGORY	Authentication
ALIENVAULT SENSOR	[REDACTED]	SUB-CATEGORY	Logout
DEVICE IP	[REDACTED]	DATA SOURCE NAME	AlienVault HIDS-syslog
EVENT TYPE ID	5502	DATA SOURCE ID	7001
UNIQUE EVENT ID#	383b11e8-b2f5-000c-295c-e65b7cd26bc4	PRODUCT TYPE	Operating System
PROTOCOL	TCP	ADDITIONAL INFO	N/A

ACTIONS

- Delete
- Create Ticket
- Insert Into DS Group
- Edit Event Properties
- Learn More

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
1	1	LOW (0)	0

SOURCE

Hostname: stable	Location: N/A
MAC Address: N/A	Context: N/A
Port: 0	Asset Groups: N/A
Latest update: N/A	Networks: Pvt_172
Username & Domain: N/A	Logged Users: N/A
Asset Value: 2	OTX IP Reputation: No

SERVICE ▲ PORT ▼ PROTOCOL ⇅

No services available

SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST

DESTINATION

Hostname: stable	Location: N/A
MAC Address: N/A	Context: N/A
Port: 0	Asset Groups: N/A
Latest update: N/A	Networks: Pvt_172
Username & Domain: N/A	Logged Users: N/A
Asset Value: 2	OTX IP Reputation: No

SERVICE ▲ PORT ▼ PROTOCOL ⇅

No services available

SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST

Optional Fields Area

USERNAME	USERDATA1	USERDATA2	USERDATA3	USERDATA4
root	/var/log/auth.log	Login session closed.	pam.syslog,	None

RAW LOG

```

AV - Alert - "1522868878" --> RID: "5502"; RI: "3"; RG: "pam.syslog."; RC: "Login session closed."; USER: "None"; SRCIP: "None"; HOSTNAME: "stable"; LOCATION: "/var/log/auth.log"; EVENT: "[INIT]Apr 4 15:07:57 stable sudo: pam_unix(sudo:session): session closed for user root[END]";
    
```

Event Detail Fields (order as appeared on the web UI)

Fields	Description
Date	Date and time of the event.
AlienVaultSensor	Sensor that processed the event.
Device IP	IP address of the USM Appliance Sensor that processed the event.
Event Type ID	ID assigned by USM Appliance to identify the event type.
Unique Event ID#	Unique ID number assigned to the event by USM Appliance.

Event Detail Fields (order as appeared on the web UI) (Continued)

Fields	Description
Protocol	Protocol used for the source/destination of the event, for example, TCP IP.
Category	Event taxonomy for the event, for example, Authentication or Exploit.
Sub-Category	Subcategory of the event taxonomy type listed under Category. For example, this would be Denial of Service, if the category were Exploit.
Data Source Name	Name of the external application or device that produced the event.
Data Source ID	ID associated with the external application or device that produced the event.
Product Type	Product type of the event taxonomy, for example, Operating System or Server.  Note: Events with IP Reputation-related data have product types; OTX pulses do not.
Additional Info	If the event were generated by a suspicious URL, for example, this field would state URL. When present, these URLs provide additional background information and references about the components associated with the event.
Priority	Priority ranking, based on value of the event type. Each event type has a priority value, used in risk calculation.
Reliability	Reliability ranking, based on the reliability value of the event type. Each event type has a reliability value, which is used in risk calculation.
Risk	Risk level of the event: Low = 0, Medium = 1, High > 1  Note: Risk calculation is based on this formula: $\text{Asset Value} * \text{Event Reliability} * \text{Event Priority} / 25 = \text{Risk}$ <p>If Asset Value = 3, Reliability = 2 and Priority = 2, the risk would be $3 * 2 * 2 / 25 = 0.48$ (rounded down to 0)</p> <p>Therefore, Risk is Low</p>
OTX Indicators	Number of indicators associated with an IP Reputation or OTX pulse event.

Event Detail Fields (order as appeared on the web UI) (Continued)

Fields	Description
Source / Destination	<p>IP addresses and hostname for the source and destination, respectively, of the event. If the host is an asset, you can right-click it to go to the Asset Details page for information.</p> <p>Right-clicking the IP address displays a menu from which you can select information about the IP, such as all events originating from that host or all events for which the IP is the destination.</p>
Hostname	<p>Hostname of the event source/destination.</p> <p>If the source or destination hostname for an event is within your asset inventory, this field contains a value. You can click it to go to the Asset Details page for more information.</p>
MAC Address	Media Access Control (MAC) of the host for the event, if known.
Port	External or internal asset source/destination port for the event.
Latest Update	The last time USM Appliance updated the asset properties.
Username & Domain	Username and domain associated with the asset that generated the event.
Asset Value	Asset value of the asset source/destination if within your asset inventory.
Location	If the host country of origin is known, displays the national flag of the event source or destination.
Context	If the asset belongs to a user-defined group of entities, USM Appliance displays the contexts.
Asset Groups	<p>When the host for the event source/destination is an asset belonging to one or more of your asset groups, this field lists the asset group name or names.</p> <p>You can click the field to go to the Asset Details page for more information.</p>
Networks	<p>When the host for the event source/destination is an asset belonging to one or more of your networks, this field lists the networks.</p> <p>You can click the field to go to the Network Group Details page for more information.</p>

Event Detail Fields (order as appeared on the web UI) (Continued)

Fields		Description
	Logged Users	A list of any users who have been active on the asset, as detected by the asset scan, for example, with the username and user privilege (such as admin).
	OTX IP Reputation	(Yes/No) Whether or not IP Reputation identifies the IP address as suspicious.
	Service	List of services or applications detected on the source/destination port.
	Port	Port used by the service or application.
	Protocol	Protocol used by the service or application.
Raw Log		Raw log details of the event.



When you see **N/A** displayed for a certain field, it means that USM Appliance has no related data in the event log or the asset inventory.

When event data derives from a log or the asset inventory, some of the fields below appear after Service, Port, and Protocol and above the Raw Log data. (See screenshot above.) Otherwise, these fields do not display.

Optional Event Fields

Fields	Description
Filename	Name of file associated with the event.
Username	The username associated with the event.
Password	The password associated with the event.
Userdata 1-9	User-created log fields.
Payload	Payload of the event.
Rule Detection	AlienVault NIDS rule used to detect the event.

There are some actions you can perform directly from the event details page.

Actions on Event Details

Actions	Description
Delete	Delete the event.
Create Ticket	Create a ticket in USM Appliance based on the event.
Insert Into DS Group	Add this event type into an existing data source group.
Edit Event Properties	Change the default priority and/or reliability value of this event type so that the calculated risk will differ. Changes will apply to future events.
Learn More	Launches the Knowledge Base information for this event.

Back Up and Restore Events

USM Appliance uses internal caches to ensure that communication interruptions between the USM Appliance Sensor and USM Appliance Server do not result in event loss. The USM Appliance Sensor collects parsed log data using the `agent_event` cache, which is stored in `/var/ossim/agent_events/`, to ensure data consistency. If a sensor loses connectivity to the server, it will continue to write to these cache files to prevent event loss. Once the sensor reconnects, it will begin forwarding from this cache again, submitting events to the server for correlation.

USM Appliance Server, on the other hand, stores security events in two different tables:

- Event table — all security events
- Alarm table — security events associated with alarms only

The backup and restore procedure described below only affects the event table. The events in the alarm table remain unchanged, therefore they remain visible in the alarm that they are associated with.

By default, USM Appliance stores security events for up to 90 days or 40 million events. When either limit is reached, USM Appliance purges older events from the database to save disk space. You can change those limits based on how many events you receive every day. You can also filter events through policies. For instructions, see "Configuring a Policy to Discard Events" in the Policy Management section of the *USM Appliance User Guide*.

Event Backup Configuration

Event backups are enabled by default. In USM Appliance version 5.4, AlienVault added a new parameter, `backup_events_min_free_disk_space`, to set the minimum free disk space required for event backup to take place. The default is 10%. If the free disk space on the system is less than this setting, event backup will not start.

To change any of the default values for event backups:

1. From the USM Appliance web UI, go to **Configuration > Administration > Main > Backup**.

2. Change the **Allowed free disk space for the SIEM backups**, if desired.

Available values are 10% and 15%. Default is 10%.

3. Change the **Number of Backup files to keep in the filesystem**, if desired.

USM Appliance keeps one backup file per day for event backups. Default is 30.

4. Change the **number of days** to keep events in the database, if desired.

0 means that there are no backup for events. Default is 90.

5. Alternatively, change the **number of events** you want to keep, if desired.

0 means that there is no limit to store events in the database. Default is 40,000,000



Important: AlienVault discourages setting either limit to 0 because you may soon run out of disk space.

ADMINISTRATION

USERS MAIN BACKUPS

BACKUP ▲

Backup configuration: backup database, directory, interval

Enable SIEM database backup	Yes ▾	?
Allowed free disk space for the SIEM backups	10% ▾	?
Number of Backup files to keep in the filesystem	30	?
Events to keep in the Database (Number of days)	90	?
Events to keep in the Database (Number of events)	400000000	?
Backup start time	01:00	?

6. Click **Update Configuration**.

Restoring Events

USM Appliance backs up events every day and place the backup files in `/var/lib/ossim/backup`. By default, it keeps 30 backup files, which correspond to 30 days of events. You can restore the events generated on a certain day.

 **Important:** If you are running USM Appliance version 5.6 or later, you cannot restore event backup files from an earlier version. This is due to a schema change in the SIEM database introduced in USM Appliance version 5.6, making the backup files from earlier versions incompatible.

To restore events from the USM Appliance web UI:

1. Go to **Configuration > Administration > Backups > Events**.
2. Select the date you want to restore.

The screenshot shows the 'ADMINISTRATION' section with 'BACKUPS' selected. Under 'EVENTS', there is a 'VIEW BACKUP LOGS' button. The 'BACKUP MANAGER' section has two columns: 'DATES TO RESTORE' and 'DATES IN DATABASE'. The 'DATES TO RESTORE' column contains a list of dates from 23-06-2016 to 17-06-2016. Below this list are dropdown menus for 'All Users' and 'All Entities', and a 'RESTORE' button. The 'DATES IN DATABASE' column contains the date 07-06-2016. Below this column is a 'CLEAR SIEM DATABASE' button. To the right, the 'LATEST BACKUP EVENTS' table shows a single entry:

USER	DATE	ACTION	STATUS	PERCENT
admin	2016-06-24 02:34:31	Insert events from 2016-06-22 to 2016-06-22	Done	100%

3. Click **Restore**.

You can click **View Backup Logs** to see the latest logs concerning backups. For example:

The 'VIEW BACKUP LOGS' window shows the following logs:

DATE	BACKUP TYPE	STATUS	MESSAGE
2017-03-03 07:00:00	Configuration	ERROR	Password for configuration backups was not set. Backups will be disabled...
2017-03-03 01:00:30	Events	INFO	Running delete: CALL alienvault_siem.fill_tables('1900-01-01 00:00:00', '2017-02-07 00:00:00')
2017-03-03 01:00:30	Events	INFO	-- Total events to delete: 0
2017-03-03 01:00:30	Events	INFO	Backup file has been compressed
2017-03-03 01:00:30	Events	INFO	Running Backup for day acid_event_2017-03-02 OK
2017-03-03 01:00:30	Events	INFO	Running Backup for day idm_data_2017-03-02 OK
2017-03-03 01:00:30	Events	INFO	Running Backup for day extra_data_2017-03-02 OK
2017-03-03 01:00:30	Events	INFO	Running Backup for day reputation_data_2017-03-02 OK
2017-03-03 01:00:30	Events	INFO	Running Backup for day otx_data_2017-03-02 OK
2017-03-03 01:00:30	Events	INFO	New backup file: /var/lib/ossim/backup/insert-20170302.sql

If the **Dates to Restore** is empty, that means all events are already in the SIEM database. You shall see the dates listed under **Dates in Database** instead.

BACKUP MANAGER

DATES TO RESTORE	DATES IN DATABASE
-- NONE --	10-05-2018 09-05-2018 08-05-2018 07-05-2018 06-05-2018 05-05-2018 04-05-2018 03-05-2018 02-05-2018 01-05-2018
<input type="text" value="- All Users -"/>	
<input type="text" value="- All Entities -"/>	
<input type="button" value="RESTORE"/>	

Clear All Events from the SIEM Database

USM Appliance backs up events every day and purges them after a threshold ([Event Backup Configuration](#)). But sometimes you may want to clear the entire database to start fresh again. For example, after the initial deployment and benchmarking exercise ([Establishing Baseline Network Behavior](#)), you may have concluded that all events in the database are noise. After configuring policies and making sure they are effective, you want a clean database to receive new events. In this case, you can clear existing events from the SIEM database manually.



Important: For compliance reasons, you may need to keep all events for a number of days. If you are not sure, consult your compliance officer.

To delete all the events through the web UI

1. Login to the USM Appliance web UI.
2. Go to **Configuration > Administration > Backups**.
3. Click **Clear SIEM Database**.

To delete all the events through the AlienVault Setup menu

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.

The AlienVault Setup menu displays.

2. Select **Maintenance & Troubleshooting**.
3. Select **Maintain Database**.
4. Select **Reset SIEM database**.

Event Storage Best Practices

USM Appliance stores events in a database and refers to as **SQL Storage**. USM Appliance also stores the normalized log data as Raw Logs on disk for forensic and compliance purposes as well as archival searches. You can forward Raw Logs to a separate USM Appliance Logger for remote storage and to reduce the load on the USM Appliance All-in-One.

The databases on the USM Appliance Server are responsible for:

- SIEM event and alarm storage
- Asset inventory storage
- AlienVault run-time configurations

Note: USM Appliance stores security events in two databases, *alienvault* and *alienvault_siem*, and stores other data in various different databases. The Database section in **Configuration > Deployment > AlienVault Center > System Detail** only shows the size of the AlienVault database and AlienVault SIEM database respectively, not the full database.

USM Appliance calculates the sizes from the data stored in the database. It is different from running CLI commands such as `du in /var/lib/mysql`, which calculates folder sizes instead.

The USM Appliance Logger is responsible for:

- Long-term storage
- Indexing logs for full-text searches
- Cryptographically signing logs
- Allowing access to events as raw text
- Allowing the forensic analysis of event
- Fulfilling compliance requirements for log archiving and management

In order to avoid filling up the USM Appliance databases or disk space, and to avoid any potential performance issues, AT&T Cybersecurity recommends the following best practices:

- Configure reasonable backup and storage thresholds, see [Event Backup Configuration](#).
- Enable alarm expiration and alarm lifetime, see [Alarm Backup Configuration](#).
- Enable logger expiration and set an active logger window, see [Raw Logs Backup Configuration](#).
- If needed, adjust the active NetFlow window, see [NetFlow Data Backup Configuration](#).
- If using USM Appliance All-in-One, configure a separate USM Appliance Logger to reduce its load. See [Configuring a USM Appliance Logger](#).
- Clean up system logs or caches on a regular basis, see [Purging Old System Logs or Clearing System Update Caches](#).
- If desired, clear SIEM events manually. See [Clear All Events from the SIEM Database](#).



Note: You should determine the configuration values or frequency based on environment, security, performance, and compliance requirements.

Network Data Management

In addition to security events collected from devices, there are other sources of information that can be useful in monitoring and analyzing the security of your network — packet information captured from network traffic and NetFlow capture of traffic information from communication between devices.

This section covers the following subtopics:

NetFlow Monitoring	178
NetFlow Monitoring Configuration	179
NetFlow Event Controls	189
NetFlow Troubleshooting	190
Back Up and Restore NetFlow Data	195
Capture and Examine Packets	198

NetFlow Monitoring

NetFlow is an industry-standard protocol designed by Cisco Systems that lets you capture information about network flows (communication between hosts using TCP/IP).

USM Appliance Sensors can generate NetFlow information from traffic received on mirrored ports, or network devices can send NetFlow information directly to the USM Appliance Server.

USM Appliance customers can use NetFlow collection as a part of behavior monitoring they want to perform. For example, NetFlow collection can assist users in identifying insecure services, and protocols and ports that should not be used. It can also assist in identifying traffic sources and destinations to help ensure that inbound internet traffic is limited to IP addresses residing within the DMZ.

NetFlow Fundamentals

Although originally designed to assist network administrators generate metrics for performance and utilization of their networks, NetFlow has gained increasing popularity in recent years as a vital tool for security analysis, detection and forensic investigation.

Operating systems and applications are rarely configured to log every last action they perform and, all too often, this can leave a critical gap in the forensic reconstruction of an "event" or incident. For example, applications or services may log who connected to them, but not from where, or when a session was started. In situations like these, cross referencing application and service logs against the records of network traffic to that host, can allow analysts to infer the missing information needed to fully reconstruct and understand events.

In any TCP/IP communication between two hosts or devices, the TCP session will contain two flows, one for the traffic going from host A to host B, and a second of the traffic going from host B to host A. NetFlow creates a flow record for each direction of communication within a TCP traffic session, capturing a standard set of information based on the particular version of NetFlow that is used. For example, using NetFlow version 5, flow records contain the following information about traffic sessions between hosts:

- Network Interface
- Source IP Address
- Destination IP Address
- IP Protocol

- Source port (for UDP or TCP flows, 0 for other protocols)
- Destination port (for UDP or TCP, type and code for ICMP, or 0 for other protocols)
- IP Type-Of-Service flags

This is the bare minimum information contained in a flow. Later versions of the NetFlow standard include additional supported fields. Of these additional fields, the ones most relevant to USM Appliance are:

- TCP Flags
- Total Packets in Flow
- Total Bytes in Flow
- Packets Per Second (PPS)
- Bits Per Second (BPS)
- Average Bits Per Packet (BPP)
- Duration (milliseconds)

 **Note:** USM Appliance currently supports NetFlow versions 1, 5, 7, 9, and 10 (aka IPFIX), plus sFlow versions 4 and 5. USM Appliance does not currently support JFlow or any other NetFlow versions not listed here.

NetFlow Monitoring Configuration

Many external NetFlow sources (such as routers and switches) have NetFlow capabilities already defined in their operating firmware and usually require only some minimal configuration to enable it. NetFlow collection is entirely dependent upon having visibility to traffic traversing the network, which means the routers and switches that traffic flows over. There are two ways to acquire this, with both options supported by AlienVaultUSM Appliance:

- Method 1: A network device is configured with a SPAN/Mirror port to clone all traffic to a single port, which is attached to an existing USM Appliance Sensor. The USM Appliance Sensor, connected to the SPAN port, generates NetFlow data from the observed network traffic.
- Method 2: Network devices are configured to generate NetFlow data, and then transmit it directly to USM Appliance Server (through a pseudo or "dummy" configured USM Appliance sensor). NetFlow data is sent from the NetFlow source to the dummy sensor, which transmits the NetFlow data to the USM Appliance Server.

After configuring the USM Appliance sensor, configure network devices to send NetFlow data to the USM Appliance dummy sensor. Use the same port to send NetFlow data as configured for the dummy sensor. This task is vendor-specific. Consult your network device vendor documentation for instructions on how to configure NetFlow on a network device.

These two options are not mutually exclusive, so USM Appliance deployments can incorporate both methods of NetFlow data collection and generation.

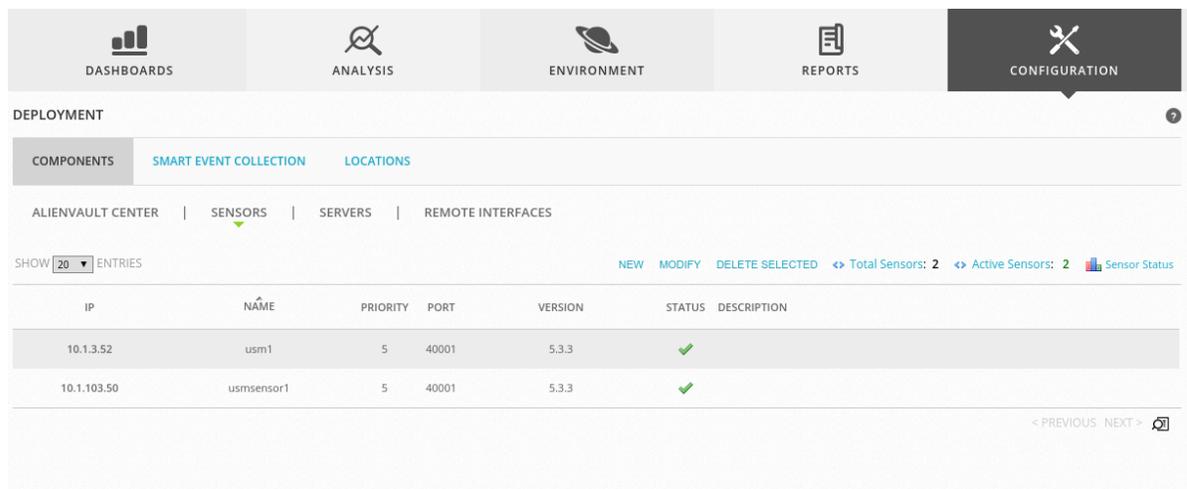
 **Important:** Be aware that when you enable NetFlow collection in USM Appliance, the flow data is kept in the file system consuming space. By default, USM Appliance stores flows for 45 days in `/var/cache/nfdump/flows`. For more information, see [Back Up and Restore NetFlow Data](#)

Enabling NetFlow Collection from an Existing USM Appliance Sensor (Method 1)

To capture NetFlow traffic information from a spanned or mirrored port, you can connect an existing USM Appliance Sensor to generate NetFlow data from the network traffic source. By default, NetFlow is disabled on USM Appliance Sensors (except for USM Appliance All-in-One), so you need to first activate and configure NetFlow collection and generation on the sensor. NetFlow collection is configured on a per-sensor basis, from the USM Appliance Sensor configuration screen:

To enable NetFlow collection from an Existing USM Appliance Sensor

1. Go to **Configuration > Deployment**.
2. Select the **Components > Sensors** tab.



The screenshot shows the USM Appliance Configuration interface. The top navigation bar includes DASHBOARDS, ANALYSIS, ENVIRONMENT, REPORTS, and CONFIGURATION. The CONFIGURATION tab is active, and the DEPLOYMENT section is expanded to show COMPONENTS, SMART EVENT COLLECTION, and LOCATIONS. The SENSORS tab is selected, displaying a table of sensors. The table has columns for IP, NAME, PRIORITY, PORT, VERSION, STATUS, and DESCRIPTION. Two sensors are listed: 'usm1' and 'usmsensor1', both with a priority of 5 and port of 40001. The STATUS column shows green checkmarks for both sensors. The interface also includes a 'SHOW 20 ENTRIES' dropdown, a 'NEW' button, and a 'DELETE SELECTED' button. The total number of sensors is 2, and the number of active sensors is 2.

IP	NAME	PRIORITY	PORT	VERSION	STATUS	DESCRIPTION
10.1.3.52	usm1	5	40001	5.3.3	✓	
10.1.103.50	usmsensor1	5	40001	5.3.3	✓	

- Click the IP Address of the sensor you want to configure to collect NetFlow source traffic information and generate NetFlow data to send to USM Appliance Server.

USM Appliance displays the main sensor configuration screen, with the NetFlow Collection Configuration detail appearing at the very bottom.

There are three primary configuration options, all of which may safely be left with their default values:

- **Port** — This is the port on which the USM Appliance Sensor will transmit NetFlow data back to the USM Appliance Server. Each sensor must transmit on a **unique** port number. A suitable default port number that you can use will appear in this text box. You can use this port unless you have a specific operational reason to choose another port, perhaps, because your network has a specific port range assigned for administrative traffic ACLs.
- **Type** — This is the type of NetFlow data that the sensor will receive from external sources. If you are only using the USM Appliance Sensor to generate NetFlow data, you can keep the default setting.



Note: Generally acceptable options are NetFlow and sFlow. In short, NetFlow provides IP flow aggregation, while sFlow provides sampled network data. Your selection of NetFlow type depends on the network device used, and its configuration. If you use Cisco or Enterasys network devices, select NetFlow. For other vendors, select sFlow.

- **Color** — A color value to visually identify flows collected from this sensor in the Flows analysis section of the USM Appliance Web UI **Environment > NetFlow** web page.
- Once you have chosen appropriate values (or kept their default settings), click **Configure and Run** to activate NetFlow collection/generation from this sensor.

The configuration section is updated to indicate that NetFlow collection for the USM Appliance Sensor is now configured.

To Enable NetFlow Generation on External Sensors

If you have added any external sensors to a USM Appliance All-in-One or other standard server installation, you need to perform one extra step to configure the internal NetFlow generation on those sensors.

1. Log into the external sensor using SSH and the credentials needed to gain access to the sensor.
2. From the Setup menu, select the **Configure Sensor > Enable NetFlow Generator** option.
3. Set the **Enable NetFlow Generator** option to **yes**.
4. Click **OK**.

You are now prompted to specify the Remote Collector Port. This is the port on which the Sensor will transmit NetFlow data back to the USM Appliance Server.

5. Specify the same port number as you selected in Step 3 of the previous procedure, [“Enabling NetFlow Collection from an Existing USM Appliance Sensor \(Method 1\)”](#).
6. Click **OK**.
7. Return to the main Setup menu and select **Apply all Changes**.
8. Exit the Setup menu and log off the sensor.

Enabling NetFlow Collection from a Dummy Sensor (Method 2)

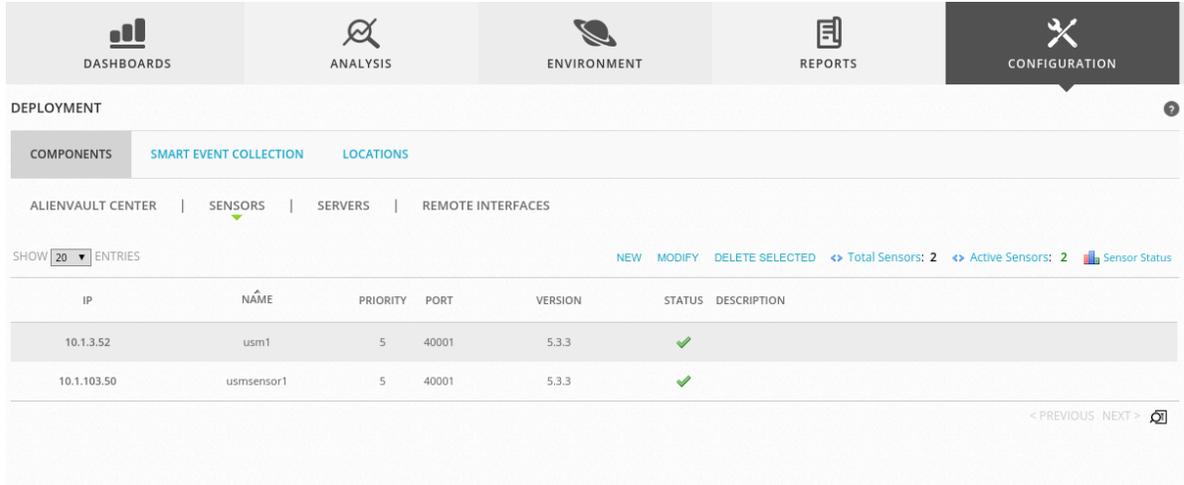
Network devices that directly support the collection, generation, and transmission of NetFlow data (or data from the variant sFlow) may also be configured as a source of NetFlow traffic information within AlienVaultUSM Appliance.

To capture NetFlow data generated by these devices, you need to create a "dummy" sensor in USM Appliance and then configure the device to transmit the NetFlow or sFlow information to the USM Appliance Server.

 **Note:** Configuring a USM Appliance "dummy" sensor just sets up a "listener" interface for the NetFlow source to send NetFlow data directly to the USM Appliance Server.

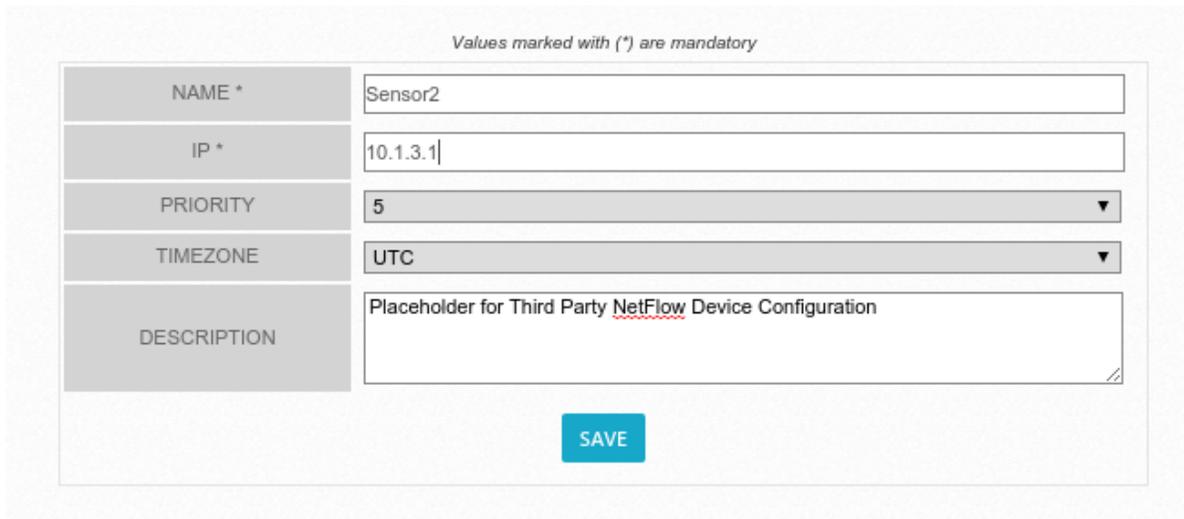
To enable NetFlow collection from a new USM Appliance dummy sensor

1. Go to **Configuration > Deployment**.
2. Select the **Components > Sensors** tab.



3. Click **New** to create a new sensor.

USM Appliance opens the sensor configuration page.



4. Specify a name and description to identify the new sensor and the IP Address of the network device sending NetFlow data to USM Appliance.
5. Click **Save**.

USM Appliance return to the **Components > Sensors** page, now listing the new sensor you just created.

The screenshot shows the Configuration page with the following structure:

- Navigation tabs: DASHBOARDS, ANALYSIS, ENVIRONMENT, REPORTS, CONFIGURATION (selected).
- DEPLOYMENT section with sub-tabs: COMPONENTS (selected), SMART EVENT COLLECTION, LOCATIONS.
- Sub-sections: ALIENVault CENTER, SENSORS (selected), SERVERS, REMOTE INTERFACES.
- Controls: SHOW 20 ENTRIES, NEW, MODIFY, DELETE SELECTED, Total Sensors: 3, Active Sensors: 2, Sensor Status.
- Table of sensors:

IP	NAME	PRIORITY	PORT	VERSION	STATUS	DESCRIPTION
10.1.3.1	Sensor2	5	40001		✗	Placeholder for Third Party NetFlow Device Configuration
10.1.3.52	usm1	5	40001	5.3.3	✓	
10.1.103.50	usmsensor1	5	40001	5.3.3	✓	

Navigation: < PREVIOUS NEXT > [refresh icon]

6. Select the new sensor you just created, and click **Modify**.
7. Scroll down the sensor configuration page to the Services section and disable all services.

The SERVICES section contains the following controls:

- AVAILABILITY MONITORING:
- VULNERABILITY ASSESSMENT:
- WIRELESS IDS:
- ACTION: UPDATE

This step is not essential, but it prevents this "dummy" sensor from showing up as an available sensor under several configuration sub-menus. When displaying a list of sensors in the USM Appliance web UI, the dummy sensor will show up in the sensor list, but will display the status as **down**, as the sensor will not respond to API requests.

8. Scroll further down the sensor configuration page to the Flows section.

The FLOWS section contains the following configuration options:

- NETFLOW COLLECTION CONFIGURATION:
 - Port: 12001
 - Color: [blue color picker]
 - Type: netflow
 - Status: is not configured
- ACTION: CONFIGURE AND RUN, Configuration help ?

There are three primary configuration options, all of which may safely be left with their default values:

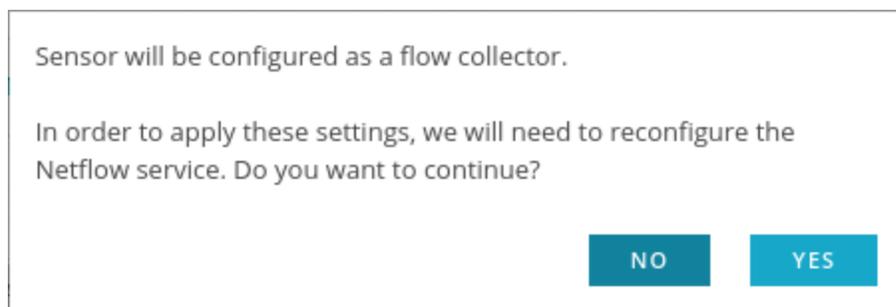
- **Port** — This is the port on which the USM Appliance Sensor will transmit NetFlow data back to the USM Appliance Server. Each sensor must transmit on a **unique** port number. A suitable default port number that you can use will appear in this text box. You can use this port unless you have a specific operational reason to choose another port, perhaps, because your network has a specific port range assigned for administrative traffic ACLs.
- **Type** — This is the type of NetFlow data that the sensor will receive from external sources. If you are only using the USM Appliance Sensor to generate NetFlow data, you can keep the default setting.



Note: Generally acceptable options are NetFlow and sFlow. Your selection of NetFlow type depends on the network device used, and its configuration. If you use Cisco or Enterasys network devices, select NetFlow. For other vendors, select sFlow.

- **Color** — A color value to visually identify flows collected from this sensor in the Flows analysis section of the USM Appliance Web UI **Environment > NetFlow** web page.
1. Once you have chosen appropriate flow configuration values (or kept their default settings), click the **Configure and Run** button to configure and activate NetFlow data collection from this sensor.

USM Appliance displays a dialog box prompting you to confirm configuration changes to the new sensor.



2. Click **Yes**.

USM Appliance applies the required sensor changes and then returns to the listing of configured sensors.



Note: After making sensor configuration changes to enable NetFlow capture, make sure that you also configure your network device to match settings specified in the sensor configuration detail. Refer to vendor documentation available for your network devices for any specific configuration required to enable or configure NetFlow data collection and generation.

Verifying NetFlow Collection

After configuring USM Appliance Sensors and network devices, you can verify USM Appliance collection of NetFlow data.



Note: Because NetFlow data collection requires capture of live network traffic, you should wait a short period (15 to 30 minutes) to allow USM Appliance time to collect a reasonable sampling of data from your network.

1. Select the **Environment > NetFlow** menu option.

USM Appliance displays the following page.



The main NetFlow web page provides three different tab selections, Details (the default), Overview, and Graph. The graphs displayed on the Details page provide a quick visual confirmation that NetFlow data is being captured. The colors used to plot the flow graphs are the colors assigned to each sensor as part of their configuration.

The Detail page also provides statistics for flows, packets, and traffic. Statistics are displayed separately for TCP, UDP, ICMP, and other protocols. The NetFlow page provides separate graphics and statistics for each NetFlow data source. In addition, you can adjust the time frame for a graph, by moving the sliders in the time line, or specifying a time range from the Display drop-down menu.

- In the middle section of the NetFlow Detail page, you can toggle the selection of statistics and graphs for data from different NetFlow sources. You can focus the display on individual flow sources by selecting a particular NetFlow source in the bottom portion of the Detail page, labelled NetFlow Processing.

Netflow Processing

LIST LAST 500 SESSIONS | TOP 10 SRC IPS | TOP 10 DST IPS | TOP 10 SRC PORT | TOP 10 DST PORT | TOP 10 PROTO

SOURCE FILTER OPTIONS

Sensor2
usmsensor1
usm1

ALL SOURCES

and <none>

List Flows Stat TopN

CLEAR FORM PROCESS

Limit to: 20 Flows

Aggregate

bi-directional
 proto
 srcPort
 dstPort

Sort:

start time of flows

Output: extended / IPv6 long

- You can further qualify NetFlow data by clicking on one of the predefined processing options, such as List Last 500 Sessions or Top 10 Src Ports, as well as selecting options from the Options section.

The following display shows a sample of results for List Last 500 Sessions.

Netflow Processing LIST LAST 500 SESSIONS | TOP 10 SRC IPS | TOP 10 DST IPS | TOP 10 SRC PORT | TOP 10 DST PORT | TOP 10 PROTO

DATE FLOW START <small>GMT-5:00</small>	DURATION	PROTO	SRC IP ADDR:PORT	DST IP ADDR:PORT	FLAGS	TOS	PACKETS	BYTES	PPS	BPS	BPP	FLOWS
2016-12-09 14:26:19.549	0.009	TCP	usm1:22	10.1.1.55:40026	.AP.S	0	4	595	444	52888	148	1
2016-12-09 14:26:19.549	0.010	TCP	10.1.1.55:40026	usm1:22	.APRSF	0	6	282	600	225600	47	1
2016-12-09 14:32:56.620	0.062	TCP	usm1:443	10.5.1.6:34617	.AP.SF	0	5	1628	80	21064	325	1
2016-12-09 14:32:56.620	0.077	TCP	10.5.1.6:34617	usm1:443	.AP.SF	0	7	605	90	62857	86	1
2016-12-09 14:32:56.569	0.069	TCP	10.5.1.6:34616	usm1:443	.AP.SF	0	7	605	101	70144	86	1
2016-12-09 14:32:56.569	0.055	TCP	usm1:443	10.5.1.6:34616	.AP.SF	0	5	1628	90	236800	325	1
2016-12-09 14:33:06.291	0.000	UDP	Host-10-1-3-54:53	usm1:47320	0	1	61	0	0	61	1
2016-12-09 14:33:06.292	0.000	UDP	Host-10-1-3-54:53	usm1:43511	0	1	50	0	0	50	1
2016-12-09 14:33:06.291	0.000	UDP	usm1:43511	Host-10-1-3-54:53	0	1	50	0	0	50	1
2016-12-09 14:33:06.292	0.000	UDP	usm1:60903	Sensor2:53	0	1	50	0	0	50	1
2016-12-09 14:33:06.290	0.000	UDP	usm1:47320	Host-10-1-3-54:53	0	1	61	0	0	61	1
2016-12-09 14:33:06.292	0.000	UDP	Sensor2:53	usm1:60903	0	1	50	0	0	50	1

You can define more specific selection criteria for NetFlow data displays in the Filter box, for example: ip x.x.x.x

Netflow Processing LIST LAST 500 SESSIONS | TOP 10 SRC IPS | TOP 10 DST IPS | TOP 10 SRC PORT | TOP 10 DST PORT | TOP 10 PROTO

DATE FLOW START <small>GMT-5:00</small>	DURATION	PROTO	SRC IP ADDR:PORT	DST IP ADDR:PORT	FLAGS	TOS	PACKETS	BYTES	PPS	BPS	BPP	FLOWS
2016-12-09 14:33:06.291	0.000	UDP	Host-10-1-3-54:53	usm1:47320	0	1	61	0	0	61	1
2016-12-09 14:33:06.292	0.000	UDP	Host-10-1-3-54:53	usm1:43511	0	1	50	0	0	50	1
2016-12-09 14:33:06.291	0.000	UDP	usm1:43511	Host-10-1-3-54:53	0	1	50	0	0	50	1
2016-12-09 14:33:06.290	0.000	UDP	usm1:47320	Host-10-1-3-54:53	0	1	61	0	0	61	1
2016-12-09 14:33:34.615	0.000	UDP	Host-10-1-3-54:53	usm1:56530	0	2	164	0	0	82	1
2016-12-09 14:33:34.614	0.000	UDP	usm1:56530	Host-10-1-3-54:53	0	2	120	0	0	60	1
2016-12-09 14:33:34.671	0.000	UDP	Host-10-1-3-54:53	usm1:51326	0	2	164	0	0	82	1
2016-12-09 14:33:36.602	0.002	TCP	usm1:514	Host-10-1-3-54:22761	.A...	0	14	560	7000	2.2M	40	1
2016-12-09 14:33:34.671	0.000	UDP	usm1:51326	Host-10-1-3-54:53	0	2	120	0	0	60	1

You can find more filter examples at <http://biot.com/capstats/bpf.html>.

NetFlow Event Controls

You are able to configure USM Appliance All-In-One to create events when anomalous bandwidth usage is detected in NetFlow data. NetFlow events are displayed under the Event Name **AlienVault-NetFlow**. NetFlow Event tracking is only available if the NetFlow is enabled and the *av-nf-alert* plugin is enabled at a Sensor level. To enable the NetFlow, see also: [Enabling NetFlow Collection from an Existing USM Appliance Sensor \(Method 1\)](#) . To learn more about enabling plugins at the Sensor level, see "Enabling Plugins from the USM Appliance Sensor Configuration" in the Plugin Management section of the *USM Appliance Deployment Guide*.

To enable events for NetFlow

1. Go to **Configuration > Administration**.
2. Select the **Main** tab and click to expand the **NetFlow** section.
3. Fill in the threshold values for the NetFlow event settings to designate the bandwidth usage that will trigger an event for an asset. The threshold's maximum and minimum values will apply to all assets on the sensor. A value of 0 in any of the fields will result in no event generation for the option in that field.

Actual Netflow threshold values will depend on your individual settings and needs.

NETFLOW ▲

Set thresholds to create events on anomalous bandwidth usage in your environment (values are in MB)

TCP Maximum Download	<input type="text" value="0"/>	?
TCP Maximum Upload	<input type="text" value="0"/>	?
UDP Maximum Download	<input type="text" value="0"/>	?
UDP Maximum Upload	<input type="text" value="0"/>	?
Inspection window (hours)	<input type="text" value="0"/>	?
If enabled, summarizes traffic by remote IP	<input type="text" value="No"/>	

4. Once the desired NetFlow event settings are completed, click the **Update Configuration** button at the top of the page to save your changes.

NetFlow Troubleshooting

If flow data from various NetFlow sources does not appear after a reasonable amount of time, you need to validate that flow data is successfully being transmitted and received by the USM Appliance Server. This section provides some specific procedures you can follow to troubleshoot NetFlow data generation, collection, and display.

Check that basic system services are running

There are several components involved in the NetFlow generation and collection process. The basic system services that are involved are the following:

- `nfсен`
- `nfсapd`
- `fprobe`(if using aUSM Appliance Sensor to generate the flows from a spanned/mirrored port)

The display of NetFlow graphics in the USM Appliance web UI is provided by `nfсен`. When you select **Environment > NetFlow** in the USM Appliance web UI and you get errors like `nfсend connect() error` or `nfсend connection failed`, this usually occurs because the `nfсен` process is not running. In that case, you will have to SSH into the system and start `nfсен` with the `service nfсен start` command. If there is a configuration error, the command will return an error message and `nfсен` won't start.

Once `nfсен` is started, you will see `nfсapd` started as well, which captures the flows. There should be one `nfсapd` process running for each sensor that has NetFlow enabled, as listed on the Administration > Deployment > Sensors page. Each `nfсapd` process will listen for flows on the port number configured for NetFlow collection on the sensor's NetFlow configuration page in the USM Appliance web UI.

NetFlow can either come from external devices that have a dummy sensor configured to collect NetFlow data, or an AlienVault Sensor configured to generate NetFlow data from a spanned/mirrored port. In the first case, you will need to create a dummy sensor and enable it for NetFlow collection. Then, you need to configure the external device to send flows to USM Appliance on the same port number as configured for that dummy sensor.

If both `nfсен` and `nfсapd` are running but there is no data displayed when you go to the **Environment > NetFlow** web page, perform the following checks.

Verify that NetFlow data files are being created daily for each sensor

The `nfсapd` process for each sensor writes the flows in a separate directory. You can see the directories by executing the command `ps auxww | grep nfсapd` and looking for the value of the parameter `'-l'` in the desired `nfсapd` process. For example:

```
ps auxww | grep nfсapd
```

```
www-data 25860 0.0 0.0 15756 704 ? S 14:53 0:00 /usr/bin/nfcapd -w -D -p 555 -
u www-data -g www-data -B 200000 -S 7 -P /var/nfsen/run/p555.pid -I
564DD32C920DB9686BDCCBBC75CD7822 -l
/var/cache/nfdump/flows//live/564DD32C920DB9686BDCCBBC75CD7822
```

Under that directory there should be several directories, one per day:

```
ll /var/cache/nfdump/flows/live/564DD32C920DB9686BDCCBBC75CD7822
.....
drwxr-xr-x 2 www-data www-data 12288 Oct 6 11:26 2014-10-04
drwxr-xr-x 2 www-data www-data 4096 Oct 6 11:41 2014-10-05
drwxr-xr-x 2 www-data www-data 4096 Oct 6 16:10 2014-10-06
-rw-r--r-- 1 www-data www-data 276 Oct 6 16:10 nfcapd.current
```

Each directory will contain flow files from the current day. One other important thing to note is that the `nfdump` command can be used to read the flows files, for example, executing the following command:

```
nfdump -r nfcapd.xxxxxxx
```

When you execute this command, do you see data in the files written by `nfcapd`? If there is data, but it does not appear in the USM Appliance web UI, it is usually because you have selected a wrong time range.

Verify that nfcapd processes are getting packets

If NetFlow data files are written, but they don't contain any information, you should check if `nfcapd` processes are getting packets. To do this, you could run the following command:

```
tcpdump -i any port <PORT>
```

If there is no communication on that port, you need to know if the flow's source is a USM Appliance Sensor or another device. If NetFlow data is coming directly from a network device that is generating the NetFlow data, you need to configure that device to send the flows to the dummy sensor. You may also want to check if there is a firewall blocking communication between the network device and USM Appliance.

As previously mentioned, a USM Appliance Sensor can generate NetFlow data by itself, when configured to listen on a SPAN/mirrored port. In this case, if you don't see traffic on the `nfcapd` port, you need to check the sensor's NetFlow configuration. The `fprobe` process listens on the interface port, takes the connection's meta information, and sends it to `nfcapd`. If you run the command `ps auxww | grep fprobe`, you will see the interface where each `fprobe` instance is listening and also the `ip:port` where `fprobe` is sending the information. For example:

```
root 26181 0.0 0.1 47420 6316 ? Ssl 14:53 0:04 /usr/sbin/fprobe -iany -fip
192.168.73.150:555
```

This command specifies the `ip:port` where `nfcapd` is listening. The IP is set to the framework machine, but the port is configurable, either through the USM Appliance web UI or the `alienvault-setup` program (**Configure Sensor > Enable NetFlow Generator > yes** and then set the desired port).

Validate that NetFlow packets are being generated by the USM Appliance Sensor

If you are collecting NetFlow packets from a third-party device (using a dummy USM Appliance Sensor), perform whatever troubleshooting is appropriate to determine that NetFlow collection is functioning correctly on that device. For sources that are using a USM Appliance Sensor to monitor network traffic and generate NetFlow data from a SPAN/mirrored port, you can follow these steps to validate that NetFlow packets are being generated by the USM Appliance Sensor:

1. SSH into the USM Appliance Sensor.
2. Launch the AlienVault Console and select the **Jailbreak System** option to access the command line.
3. Run the following command to validate that `fprobe` is running, that it is listening to the correct interface, and that it is sending packets on the correct port to the USM Appliance Server.

```
# ps ax|grep fprobe
```

The output from this command should appear similar to the following:

```
1923 ?          ss1    7:04 /usr/sbin/fprobe -ieth1 -fip 192.168.1.240:12000
```

4. Confirm that `-iethX` is the correct interface number for the sensor interface connected to the switch SPAN port.
5. Confirm that the IP address returned is the IP address of the USM Appliance Server.
6. Confirm that the port number (following the IP address) is the same number you specified in the USM Appliance web UI for the NetFlow configuration.

Checking other possible reasons that `nfcapd` processes are not receiving NetFlow data

If everything appears to be correctly configured; you see some traffic between `fprobe` and `nfcapd` and the NetFlow directory files are written, but running the `nfdump` command indicates the `nfcapd` process still isn't receiving NetFlow data, the problem may be due to the following:

The sensor is not configured to listen using the correct interfaces. (**Check Configure Sensor > Configure Network Monitoring**).

- The sensor is not configured to listen using the correct interfaces. (Check **Configure Sensor > Configure Network Monitoring**.)
- The interface is not receiving traffic (usually due to faulty configuration of the port mirroring). You could check the configuration with the command `tcpdump -i <interface>`.
- The interface is receiving traffic, but it is not purely IP traffic. For example, if the interface is receiving tagged VLAN traffic, `fprobe` is not going to capture the traffic, because generation of NetFlow data from VLAN traffic is not supported. To check if you are monitoring purely IP traffic, you can run the command `tcpdump -i <interface> ip`.

Validate that NetFlow packets are being received by the USM Appliance Server

1. SSH into the USM Appliance Server.
2. Launch the AlienVault Console and select the **Jailbreak System** option to access the command line.
3. Validate that `nfcapd` is running, and listening on the port assigned for the appropriate sensor, by running the following command:

```
# ps ax|grep nfcapd
```

The output should appear similar to the following:

```
2893 ?        S          0:00 /usr/bin/nfcapd -w -D -p 12001
2899 ?        S          0:03 /usr/bin/nfcapd -w -D -p 12000
```

- There will be multiple instances of `nfcapd`, one for each NetFlow source.
 - The number after the `-p` argument should match the port assigned to a particular NetFlow source.
4. Use `tcpdump` to validate that packets are being transmitted to the USM Appliance Server.

```
# tcpdump -I <interface> 'port <netflow port>'
```

If packets are being received from the NetFlow source, you should see output similar to the following:

```
alienvault-server:~# tcpdump -i eth0 'port 12000'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
18:48:01.056887 IP 192.168.1.241.41476 > alienvault-server.alienvault.12000: UDP, length 216
18:48:06.053524 IP 192.168.1.241.41476 > alienvault-server.alienvault.12000: UDP, length 312
18:48:11.059557 IP 192.168.1.241.41476 > alienvault-server.alienvault.12000: UDP, length 696
```

5. Use Ctrl-C to exit `tcpdump`.

Validate that NetFlow packets are accepted by the USM Appliance Server Firewall

1. SSH into the USM Appliance Server.
2. Launch the AlienVault Console and select the **Jailbreak System** option to access the command line.
3. Validate that the firewall configuration has an exception configured to allow incoming NetFlow data packets over the appropriate UDP port.

```
# iptables -L -n -v |grep <configured port>
```

The output should resemble the following:



```
alien@alienvault-server:~# iptables -L -n -v |grep 12000
33482 21M ACCEPT udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:12000
```

The `udp dpt` segment (destination port) is the important part here, indicating that traffic will be **ACCEPT**ed by the firewall configuration. The number in the left column indicates the number of packets that have previously matched this **ACCEPT** rule.

Back Up and Restore NetFlow Data

NetFlow is a protocol designed and published by Cisco Systems that has become the accepted industry standard for recording and transmitting information about network flows. Through AlienVault USM Appliance you can back up and restore the information about flows in a network.

NetFlow Data Backup Configuration

To configure the backup of NetFlow data

1. From the USM Appliance web interface, go to **Configuration > Administration > Main > Backup**.
2. Set the number of days to store flows in the **Active NetFlow Window** field. Default is 45

days.

ADMINISTRATION

USERS MAIN BACKUPS

BACKUP ▲

Backup configuration: backup database, directory, interval

Enable SIEM database backup	Yes ▾	?
Number of Backup files to keep in the filesystem	30	?
Events to keep in the Database (Number of days)	90	?
Events to keep in the Database (Number of events)	40000000	?
Backup start time	01:00	?
Active Netflow Window	45	?
Alarms Expire	No ▾	?
Alarms Lifetime	0	?
Logger Expiration	Yes ▾	?
Active Logger Window	365	?
Password to encrypt backup files		?

3. Click **Update Configuration**.

Backing Up NetFlow Data

To back up NetFlow data

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
2. On the AlienVault Setup main menu, select **Jailbreak System** to gain command line access.

Select **Yes** when prompted. You will be in the root directory.

3. On the command line, type the following command:

```
screen
```

We recommend using the screen session so that you can keep the program running even after you log out.

4. Run the following command:

```
tar czf alienvault-netflow-`date +%s`.tgz /var/nfsen /var/cache/nfdump
```

Adding ``date +%s`` to the filename gives it a unique time stamp.

This procedure creates the `alienvault-netflow-<timestamp>.tgz` file. Transfer the file to the target system. You can use either an SFTP client on Windows, such as WinSCP; or the SCP protocol on Linux.

Restoring NetFlow Data

Before following the procedure below, you should have deployed the SAME version of USM Appliance. You should have transferred the backup files to the target system and place them in the root directory.

To restore NetFlow data

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.

The AlienVault Setup menu displays.

2. On the AlienVault Setup main menu, select **Jailbreak System** to gain command line access.

Select **Yes** when prompted. You will be in the root directory.

3. On the command line, type the following command:

```
screen
```

We recommend using the screen session so that you can keep the program running even after you log out.

4. Stop the following services so that they do not interfere with the process:

```
/etc/init.d/monit stop
/etc/init.d/ossim-server stop
/etc/init.d/ossim-agent stop
/etc/init.d/ossim-framework stop
/etc/init.d/alienvault-api stop
```

5. Extract the backup file into the '/' directory:

```
tar xvzf alienvault-netflow-<timestamp>.tgz -C /
```

6. Update file permissions:

```
tar tvzf alienvault-netflow-<timestamp>.tgz | tr -s ' ' > /root/file_list
ulimit -s 65536
cd /
```

```
for i in `cat /root/file_list | cut -f2 -d" " | sort -u`; do user=`echo $i  
| cut -f1 -d"/"`; group=`echo $i | cut -f2 -d"/"`; chown $user:$group  
`grep $i root/file_list | cut -f6 -d" " | xargs`; done  
ulimit -s 8192
```

7. Restart all services for changes to apply:

```
alienvault-reconfig -c -v -d
```

Capture and Examine Packets

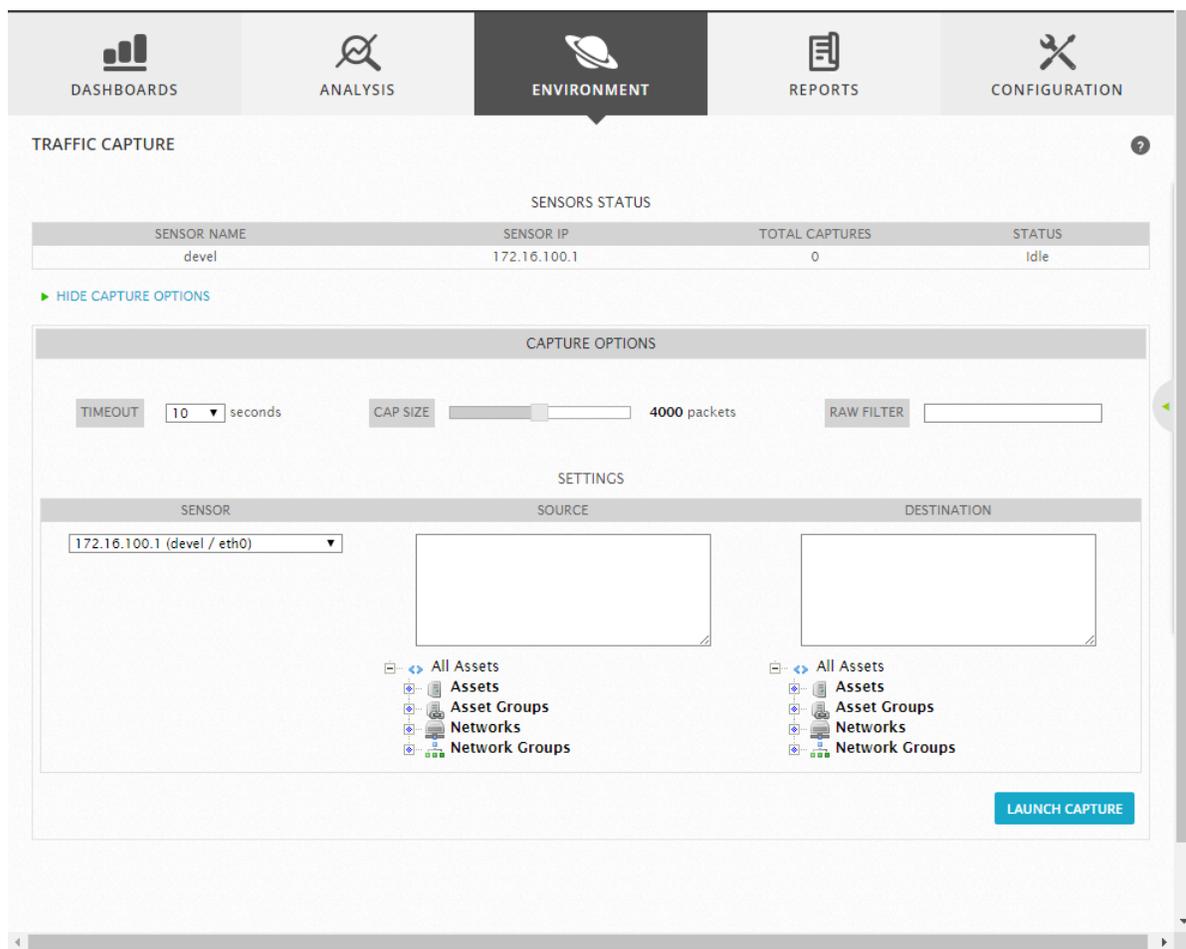
AlienVault USM Appliance integrated packet capture functionality allows you to capture traffic on your network for offline analysis and forensics, using the USM Appliance web UI.



Note: You can also perform traffic captures through the system shell, for example, using TcpDump or Tshark.

To capture a packet

1. Go to **Environment >Traffic Capture**.



2. Select how long, in seconds, the capture should operate, using the **Timeout** filter.
Timeouts are 10, 20, 30, 60, 90, 120, and 180 seconds.
3. Select the number of packets to capture by sliding the **Cap Size** bar.
Numbers range from 100 to 8000.
4. Type the name for a raw filter in the **Raw Filter** field; for example, 80 (the web server port).
5. Select the sensor and the interface from which to capture packets by expanding the **Sensor** list.

6. Select the IP addresses for the source and destination of the traffic you want to capture by expanding their respective **All Assets** trees, below the **Source** and **Destination** fields.

When you select the host IPs, **Source and Destination** is populated.

7. Click **Launch Capture**.

The system informs you that it is starting the capture.

When USM Appliance has captured the packets, it displays a Traffic Capture results page that reports the capture start time, the duration, the user, and the action you want to take with the capture (Delete, Download, View Payload).

After you complete the packet captures, you can examine them in the integrated GUI of Tshark, which displays in a separate browser window. You can also download the capture as a PCAP file and examine it, using any external packet capture tool, such as Wireshark.

Raw Log Management

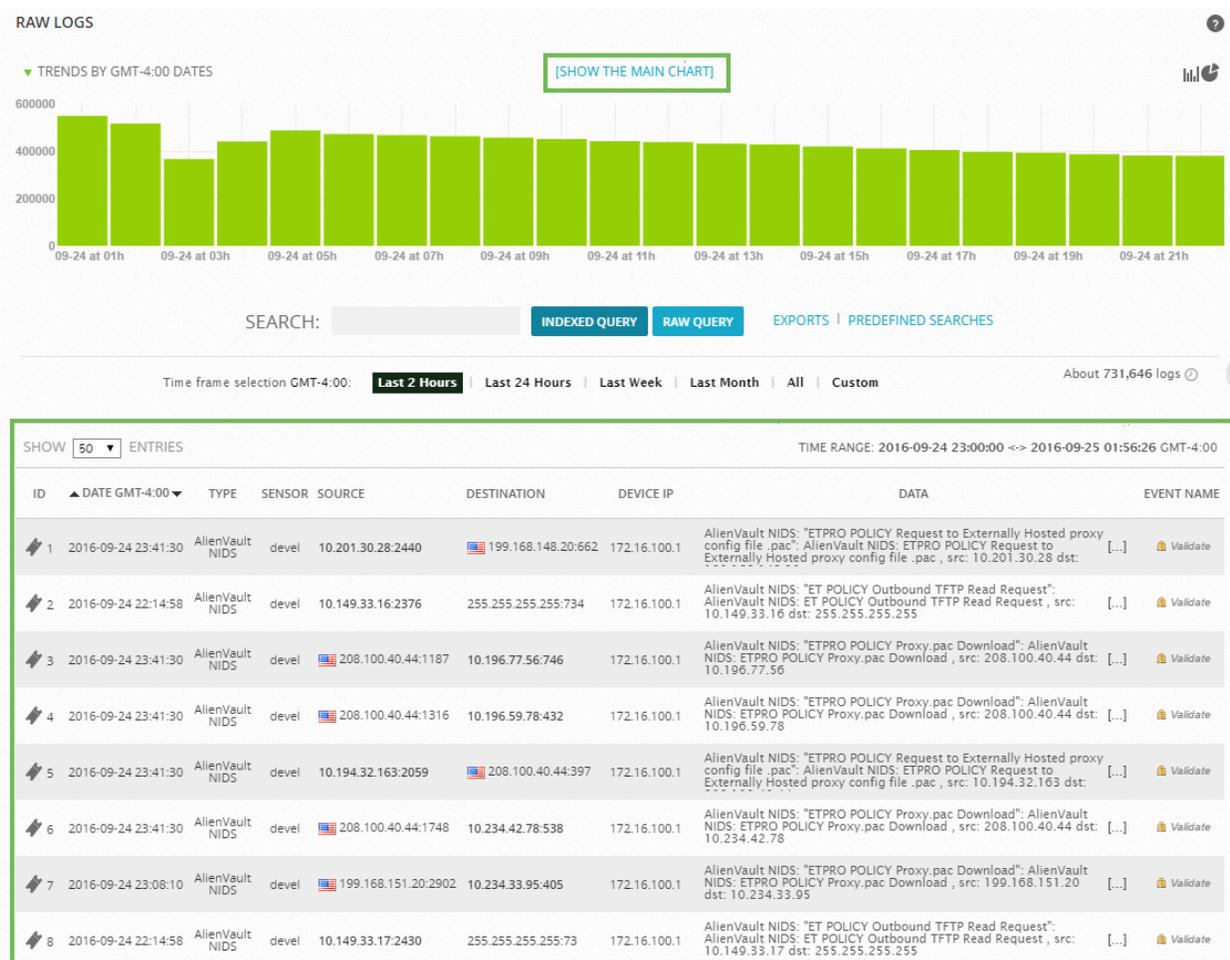
Raw logs in USM Appliance consist of event data stored in the Logger after a Sensor parses and normalizes raw data from devices, sends them to the Server, and then the Server forwards them to the Logger. The AlienVault USM Appliance Logger securely archives raw event data as logs without any filtering. Raw logs are an invaluable asset for forensic analysis and compliance mandates. You can review logs to find details about specific incidents, search the logs for instances using a specific IP address, or analyze the patterns of multiple attacks.

This section covers the following subtopics:

Raw Logs Page Overview	202
Graphs and Charts for Raw Logs	203
Search Raw Logs	205
Review and Verify Raw Logs	209
Configure the Digital Signing of Raw Logs	211
Export Raw Logs	213
Back Up and Restore Raw Logs	214

Raw Logs Page Overview

When you select the **Analysis > Raw Logs** option, USM Appliance displays the following page.



This page provides access and display of all the normalized events that the USM Appliance Logger saved to its archived log files for long-term storage and forensic investigation. The USM Appliance Logger digitally signs and timestamps the archived log files to ensure their integrity and guarantee, for compliance reporting, that the data in log files has not been tampered with. From the Raw Logs page, you can click the  icon to validate that any particular event has not been altered.

By default, the Raw Logs page displays a raw log event trending graph, which shows the number of events occurring within a specified interval of time. You can click on any of the bars to display only the events that occurred within that time frame.

The USM Appliance web UI provides another option, **Show the Main Chart**, which provides another view of raw log events. You can also click the  icon to alternate the display to a collection of pie charts that show the distribution of events by sensor, event types, sources, and destinations.

Below the trending chart, you can specify the duration of the time frame, such as last 2 hours, last 24 hours, or last week. In addition, you can specify a logical expression search string query to filter the event display. Below the trending chart, and Search areas, the web UI provides a tabular display of events matching a selected time frame, or matching an indexed or raw query.

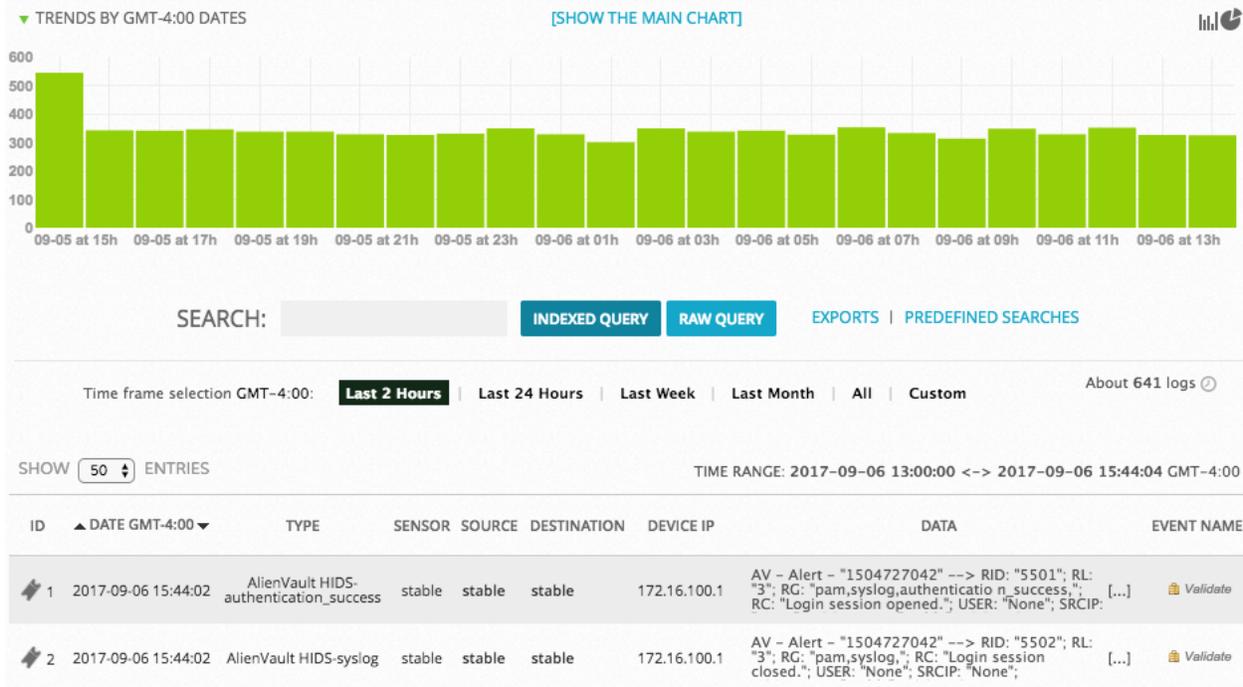
Graphs and Charts for Raw Logs

At the top of the Raw Logs page, found by navigating to **Analysis > Raw Logs**, you can find graphical representations of raw log statistics, either as bar graphs or pie charts. This is a quick and useful way for monitoring activity and event types.

Bar Graph

The bar graph shows how many logs were created and over what period of time. This indicates the trend over a specified period. By default, the graph shows the last twenty four hours of logs. However, you can select the the last week, the last month, the last year, or all of the logs in the Logger since USM Appliance was set up. You can click an individual bar of the graph to isolate the logs for that specific timeframe.

The associated logs appear in the Log list below the graph.



Pie Charts

The pie chart shows the logs on a particular sensor IP address or by event type.

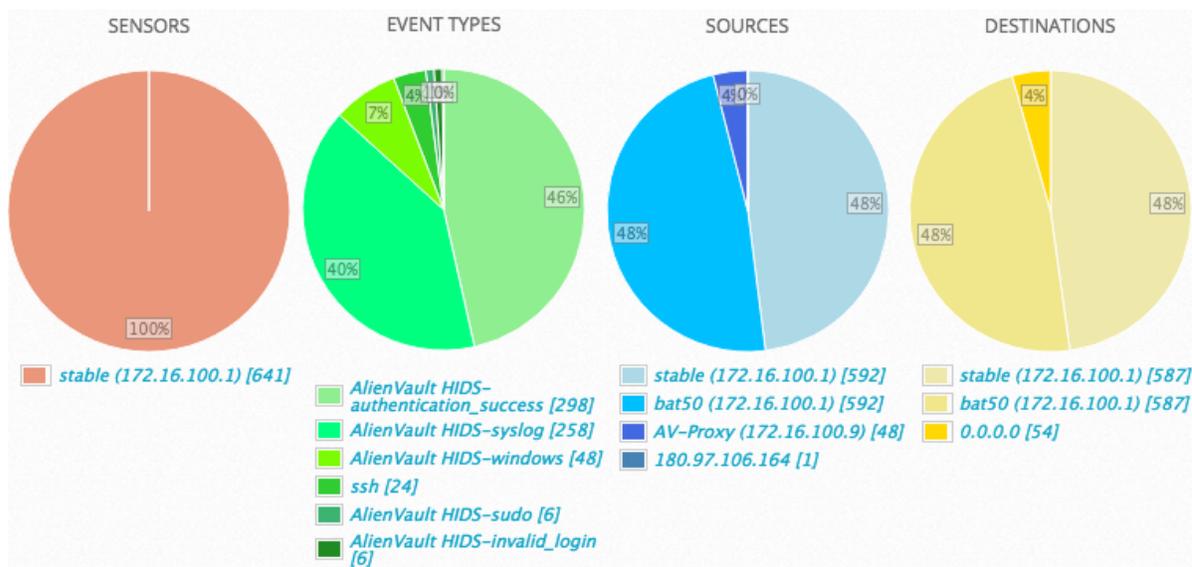
The Logger pie charts show the number of logs as a percentage of total and focusing on the following:

- **Sensors** — Shows all of the events grouped by USM Appliance Sensor IP address.
- **Event types** — Shows all of the events grouped by type.
- **Sources** — Shows all events grouped by up to 10 source IP addresses.
- **Destinations** — Shows all events grouped by up to 10 destination IP addresses.

To access the Logger pie charts

1. Click the pie chart icon () on the upper-right of the graph to open the graphs window.

- Click on any of the fields below the pie charts to populate the raw logs list with the corresponding logs.



Search Raw Logs

Raw logs can be searched for further analysis and review. Raw log searches are case-sensitive. You can perform either an indexed query or a raw query using one or more of the tags provided in this section as your search criteria.

- Indexed queries search the logs that have been indexed by USM Appliance.
- Raw queries search all logs.

For this reason, the Indexed Query is usually faster than the Raw Query. USM Appliance indexes new raw log entries on an hourly basis.

Search the Raw Logs with Indexed Query or Raw Query

To perform either an indexed or raw query

- On the Raw Logs page (**Analysis > Raw Logs**), type the case-sensitive string into the **Search** field.

As soon as you start entering a value in the **Search** field, USM Appliance displays a list of tags in the following syntax: `<tag>=<string>`, `<tag>!<string>`

For example

```
plugin=SSH, src=10.151.184.70, src_port!=80
```

- Click the appropriate tag containing your string.

Warning: You cannot enter the query as free text.

SEARCH:

Time frame selection GMT-4:00: | | | | |

If you use multiple tags, USM Appliance combines them for you and infers use of the AND operator.

For a list of valid tags, see the [Raw Log Search Tags List](#) below.

- Click either **INDEXED QUERY** or **RAW QUERY**.

INDEXED QUERY will search all the indexed fields within the logs directory. **RAW QUERY** will search the entire text logs located in `/var/ossim/logs`.

Note: If using the "data" tag, you can only click **RAW QUERY**, because the "data" tag only searches the non-indexed text.

- If you want to create a new query after completing the first one, click the "x" next to the original query to remove it or use the keyboard delete key.

Raw Log Search Tags List

Tag	Definition	Valid Input Value String
sensor	Name of a USM Appliance Sensor or Sensor in the network.	Text string or numeric string Example: ThatSensor
src	Source IP address, hostname, or network to search on.	Text string or numeric string Example: src=10.10.10.10
dst	Destination IP address, hostname, or network to search on.	Text string or numeric string Example: dst=10.10.10.10

Raw Log Search Tags List (Continued)

Tag	Definition	Valid Input Value String
IP	IP address, hostname, or network to search on.	Numeric string Example: IP=10.10.10.10
data	Greps across the DATA field constituting the raw text of the log. Can only be used in RAW QUERY search.	Alphanumeric string; special chars allowed. Example: data=preauth
plugin; datasource	Name of plugin or datasource in your network.	Text string Example: datasource=USM Appliance NIDS-spp_portscan
dsgroup; pluggingroup	Name of USM Appliance and user-created groups of datasources. Note: dsgroup and pluggingroup are synonymous.	Text string Example: dsgroup=get IP request
src_port	Source port number (integer) as defined in port table in ossim-db.	Numeric string Example: src_port=898
dst_port	Destination port number (integer) as defined in port table in ossim-db.	Numeric string Example: dst_prt=898
product_type	Device type, based on taxonomy.	Text string Example: product_type=Authentication and DHCP
category, event_ category	Event category type as defined in the category and subcategory tables in ossim-db	Text string Example: category=access-ACL Permit
username	User name, based on IDM plugin.	Case-sensitive string Example: sfukuda

Raw Log Search Tags List (Continued)

Tag	Definition	Valid Input Value String
filename	Name of any file included in the logs.	Case-sensitive string Example: survey-031415.txt
entity	Predefined user group name, typically, based on organizational structure.	Alphanumeric string; special chars allowed. Example: Accounting Dept
userdata1 ~ userdata9	Additional data fields for user input.	Case-sensitive string Options: name, username, file hash, URL, IP, and any data possibly present in a log file.

Special Characters in Search Strings

USM Appliance treats some characters as delimiters while indexing raw log entries, therefore, they cannot be used in an indexed query.

These characters include:

```
space
:
;
'
=
[
]
(
)
"
```



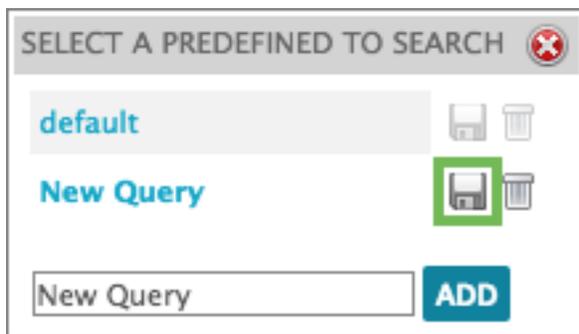
Note: A back slash ('\') or a forward slash ('/') works in both Indexes Query and Raw Query searches.

Save and Run a Query

If you have search queries that are frequently used or important, you can save them to quickly run them again as needed.

To save a query

1. Perform a search in the search field.
2. Click **Predefined Searches**.
3. In the **Select a Predefined to Search** popup, give the search a name and click **Add**.
4. Click the Diskette icon () to save the query.



To run a saved query

1. Click **Predefined Searches**.
2. In the **Select a Predefined to Search** popup, select the query name.

To delete a saved query

1. Click **Predefined Searches**.
2. In the **Select a Predefined to Search** popup, select the query you want to delete and click the Trash icon () .
3. Click **OK** to confirm deletion.

Review and Verify Raw Logs

When you examine an event, you can find additional information by examining the raw logs that the USM Appliance Logger stores. When retrieving information from the raw logs, you can perform a verification to ensure that the data has not been tampered with. This helps you meet governmental and other compliance mandates for archival and management. It also enables the forensic analysis of all events. The USM Appliance Logger signs the raw logs digitally before storing them.

 **Note:** Beginning with version 5.4, USM Appliance uses DSA (Digital Signature Algorithm), in place of SHA-1, to sign raw logs.

Because it is still possible for individuals to tamper with logs, use this procedure to verify that no one has altered any of them.

To search for raw logs related to activity in an alarm

1. Go to **Analysis > Raw Logs** and search for any raw logs related to activity that triggered an alarm.
2. Fill in the **Search** field and click either **Indexed Query** or **Raw Query**.

Indexed Query will search all the indexed fields filed within the logs directory. **Raw Query** will search the entire text logs located in `/var/ossim/logs`.

3. Click any individual log to expand its details for further information.
4. When your search returns the desired log, click **Validate**, located in the Signature column of the list.

ID	DATE GMT-4:00	TYPE	SENSOR	SOURCE	DESTINATION	DEVICE IP	DATA	EVENT NAME
1	2017-09-06 08:58:55	AlienVault HIDS-syslog	stable	stable	stable	172.16.100.1	AV - Alert - "1504702735" --> RID: RL: "3"; RG: "pam,syslog,,"; RC: "Login session closed.,"; USER: "None"; SRCIP:	

5. If the log validation is successful, a popup will display with the full log verification results.

VALIDATE SIGNATURE ✕

LOG VERIFICATION RESULTS

Logline: AV - Alert - "1504702115" --> RID: "5502"; RL: "3"; RG: "pam,syslog,,"; RC: "Login session closed.,"; USER: "None"; SRCIP: "None"; HOSTNAME: "stable"; LOCATION: "/var/log/auth.log"; EVENT: "[INIT]Sep 6 08:48:34 stable sudo: pam_unix(sudo:session): session closed for user root[END]";

Found in log file `'/var/ossim/logs/2017/09/06/12/172.16.100.1/2017-09-06T12-00-01.307183Z.log'`

DSA Verification OK

If the log was altered since its original signing, a popup will be displayed reading "Verification Failed."



Important: If your logger is set for block signing, a signature may not yet be available if the log is only one hour old. If you want to have logs signed immediately, change the configuration of the logger to perform line signing. See [Configure the Digital Signing of Raw Logs](#) for more information.

Configure the Digital Signing of Raw Logs

USM Appliance uses cryptographic signing of raw logs stored on disk for security and verification purposes. This helps you meet governmental and other compliance mandates for archive and management. It also allows for the forensic analysis of all events in USM Appliance.

 **Note:** Beginning with version 5.4, USM Appliance uses DSA (Digital Signature Algorithm), in place of SHA-1, to sign raw logs.

To certify the logs and protect them from being modified or tampered with, USM Appliance uses one of two ways to digitally sign the raw logs:

- **Line** — Digitally signs every log it receives. This ensures immediate protection from log tampering, but it can take longer to process.
- **Block** — Digitally sign a block of logs on an hourly basis, or when the log file exceeds 100 MB in size. This is the default signing method

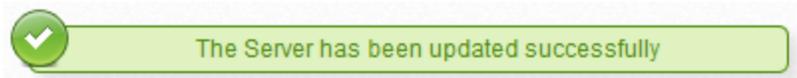
To configure the Logger's method of digitally signing logs

1. Go to **Configuration > Deployment > Components > Servers**.
2. Select a server, then select **Modify**.
3. On the Components page, in the **Log** section, verify that **Yes** is selected for **Credentials**.

NAME *	<input type="text" value="stable"/>
IP *	<input type="text" value="172.16.100.1"/>
PORT *	<input type="text" value="40001"/>
<u>SECURITY EVENTS</u> *	<input checked="" type="radio"/> Yes <input type="radio"/> No
QUALIFY EVENTS *	<input checked="" type="radio"/> Yes <input type="radio"/> No
CORRELATE EVENTS *	<input checked="" type="radio"/> Yes <input type="radio"/> No
CROSS CORRELATE EVENTS *	<input checked="" type="radio"/> Yes <input type="radio"/> No
STORE EVENTS *	<input checked="" type="radio"/> Yes <input type="radio"/> No
ALARMS TO SYSLOG *	<input type="radio"/> Yes <input checked="" type="radio"/> No
IP REPUTATION *	<input checked="" type="radio"/> Yes <input type="radio"/> No
<u>LOG</u> * ▶ CREDENTIALS	<input checked="" type="radio"/> Yes <input type="radio"/> No
SIGN *	<input type="radio"/> Line <input checked="" type="radio"/> Block
<u>MULTILEVEL</u>	<input checked="" type="radio"/> Yes <input type="radio"/> No
FORWARD ALARMS *	<input checked="" type="radio"/> Yes <input type="radio"/> No
FORWARD EVENTS *	<input checked="" type="radio"/> Yes <input type="radio"/> No
FORWARD SERVERS ▶ ADD SERVER	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div> <div style="text-align: right;"><input type="button" value="X"/></div>
DESCRIPTION	<div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div>

- Next to **Sign**, select either **Line** or **Block** for the signing method you want to use.
- Click **Save**.

This returns you to the Components tab, where USM Appliance displays the message that the server has been successfully updated.



- Click **Apply Changes**.

Export Raw Logs

Raw logs can be exported as a text file for offline analysis, backup storage, or for evidence.

To export raw logs from the USM Appliance web UI

- Go to **Analysis > Raw Logs** and search for the raw log related to the alarm you are investigating.
- After filtering your results with the search, click **Exports**.

If you have never exported any raw log files before this, USM Appliance displays, `No export files found`.

- Select either **Screen Export** or **Entire Export**.
 - Screen Export** exports only the entries displayed on the screen.
 - Entire export** exports the entire search result. When you select this, USM Appliance limits the export to 249,999 logs.
- After selecting the logs you want exported, click the **Download** icon.





Important: The Logger stores all timestamps in UTC timezone format internally, so all exports will be formatted accordingly. This is important to consider for raw log storage, search tools, and raw log backup, as the timestamps and dates on disk will follow this protocol.

For example, an security event recorded on January 20, 2017 at 22:00 EST (GMT-5) will be stored internally on disk in file located in `/var/ossim/logs/2017/01/21/03/sensor_ip/timestamp-for-logfile.log`

Back Up and Restore Raw Logs

By default, USM Appliance stores raw logs in the file system until they are deleted. AlienVault recommends that you export these files to an offline persistent storage site periodically and remove them from USM Appliance manually. You can also configure the raw logs to expire after a certain time so USM Appliance can purge them from the system automatically.

Raw Logs Backup Configuration

To configure the expiration of raw logs:

1. From the USM Appliance web interface, go to **Configuration > Administration > Main > Backup**.
2. Change **Logger Expiration** to **Yes**.

The Active Logger Windows defaults to 365 (days). This value refers to the number of days to keep the logs. 0 means that the logs never expire.

3. Change **Active Logger Window** to a suitable number based on your environment and

your company's requirement.

ADMINISTRATION

USERS MAIN BACKUPS

BACKUP ▲

Backup configuration: backup database, directory, interval

Enable SIEM database backup	Yes ▾	?
Number of Backup files to keep in the filesystem	30	?
Events to keep in the Database (Number of days)	90	?
Events to keep in the Database (Number of events)	40000000	?
Backup start time	01:00	?
Active Netflow Window	45	?
Alarms Expire	No ▾	?
Alarms Lifetime	0	?
Logger Expiration	Yes ▾	?
Active Logger Window	365	?
Password to encrypt backup files		?

4. Click **Update Configuration**.

Backing Up Raw Logs

USM Appliance store raw logs in `/var/ossim/logs` and organizes them in this order: year, month, day, hour (UTC), and USM Appliance Sensor IP. For example, to find the raw logs reported by sensor 192.168.73.159 at 10 o'clock on August 5, 2016, go to `/var/ossim/logs/2016/08/05/10/192.168.73.159`.

To back up raw logs

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
2. On the AlienVault Setup main menu, select **Jailbreak System** to gain command line access.
Select **Yes** when prompted. You will be in the root directory.
3. On the command line, type the following command:

```
screen
```

We recommend using the screen session so that you can keep the program running even after you log out.

4. For efficiency, use the `rsync` protocol to transfer the raw logs to the destination:

Syntax:

```
rsync -av --progress /src_folder_path <username>@<dest_ip_address>:<dest_folder_path>
```

Example 1: Transferring raw logs of March 2017

```
rsync -av --progress /var/ossim/logs/2017/03
root@10.10.10.10:/var/ossim/logs/2017
```

Example 2: Transferring all raw logs of 2017

```
rsync -av --progress /var/ossim/logs/2017 root@10.10.10.10:/var/ossim/logs
```



Important: Leave out the trailing slash ('/') on the source so that the corresponding directory will be created at the destination.

The raw logs should be transferred to the destined machine, in this case, `10.10.10.10`, and store in the `/var/ossim/logs` directory.

Purging Raw Logs

After backing up the raw logs and transferring them to an external storage, you need to remove them from USM Appliance manually.

To remove raw logs

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
2. Select **Maintenance & Troubleshooting**.
3. Select **Maintain Disk and Logs**.
4. Select **Purge Logger Data**.
5. Select **Delete logger entries older than a date**.
6. Enter a data in the `YYYY/MM/DD` format then press Enter `<OK>`.

USM Appliance will delete any raw logs older than the date specified.

Restoring Raw Logs

Before following the procedure below, you should have deployed the SAME version of USM Appliance. You should have transferred the backup files to the target system and place them in the root directory.

You can also restore raw logs that were archived and purged from the same USM Appliance instance in the past.

To restore raw logs

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.

The AlienVault Setup menu displays.

2. On the AlienVault Setup main menu, select **Jailbreak System** to gain command line access.

Select **Yes** when prompted. You will be in the root directory.

3. On the command line, type the following command:

```
screen
```

We recommend using the screen session so that you can keep the program running even after you log out.

4. If not done already, use the `rsync` protocol to transfer the raw logs to `/var/ossim/logs` directory.

5. Change ownership for raw logs.

Using "Example 2: Transferring all raw logs of 2017" from the backup steps above, type

```
chown -R www-data:alienvault /var/ossim/logs/searches
chown -R avserver:alienvault /var/ossim/logs/2017
```

6. Change permission for raw logs.

Using "Example 2: Transferring all raw logs of 2017" from the backup steps above, type

```
chmod -R 775 /var/ossim/logs/2017
```

Ticket Management

A ticket is a tracking tool that contains information about detected alarms or any other issues that you want to manage in a workflow. When dealing with alarms and events, the best practice is to always keep track of progress and insights into the issue by creating a ticket, either through the USM Appliance ticketing system or through your own company's ticketing system, if applicable. Not only can creating a ticket for an alarm or event help you in a future investigation, it also creates an audit trail to track what you saw, what actions were taken, and track progress on the issue.

This section covers the following subtopics:

Tickets Page Overview	219
Create a Ticket	219
Search and Close Tickets	222
Edit a Ticket	224

Tickets Page Overview

When you select the **Analysis > Tickets** option, USM Appliance displays the following page.

TICKETS

SIMPLE FILTERS [SWITCH TO ADVANCED]

Class: ALL, Type: ALL, Search text: , In charge: , Status: Open, Priority: ALL, [CLOSE SELECTED] [SEARCH]

► APPLY TAGS TO SELECTED TICKETS

TICKET	TITLE	PRIORITY	CREATED	LIFE TIME	IN CHARGE	SUBMITTER	TYPE	STATUS	EXTRA
EVE01	Welcome to AlienVault	2	2016-09-23 02:30:52	2 Days 03:28	Admin	Admin	Generic	Open	

Pag. 1

Open a new ticket manually: Alarm [CREATE]

This page provides access to the USM Appliance ticket remediation system. Tickets provide workflow tracking of activity related to detected alarms or any other issues that you want to keep track of. By default, the USM Appliance web UI displays a list of all tickets. In addition, you can click **Create** to open a new ticket of a specific type or category.

In the Filters section at the top of the page, you can choose criteria to filter the ticket results. You can choose additional criteria to filter ticket results by clicking the **Switch to Advanced** option.

From the Ticket summary list, you can click a specific ticket to display the details of the ticket on a new page. From this ticket detail display, you can perform various actions such as editing fields in the ticket, assigning the ticket, adding notes and attachments, and changing the status and priority of a ticket, depending on whatever method or process you want to use to track resolution of issues.

Create a Ticket

You can open a ticket in the following ways:

- Automatically — based on a configured policy. See [Create an Action](#) for details.
- Automatically — [as a response to a detected vulnerability](#).
- Manually — [during an alarm investigation](#).
- Manually — [unrelated to an alarm or an event](#).

Open Tickets Automatically

To have USM Appliance open tickets when a new alarm is generated

1. Go to **Configuration > Administration > Main**.
2. Expand **Tickets**.

The screenshot shows the 'TICKETS' configuration page. The title 'TICKETS' is at the top left with an upward-pointing triangle. Below it, the section is titled 'Tickets parameters'. There are five rows of configuration options, each with a help icon (a question mark in a circle) to its right:

- Open Tickets for new alarms automatically?**: A dropdown menu currently set to 'No'.
- Automatic ticket generation default in-charge user/entity**: A dropdown menu currently set to 'Admin'.
- Send email notification**: A dropdown menu currently set to 'No'.
- Open tickets reminder**: A text input field containing the number '15'.
- Email Template for tickets**: A link labeled 'Click here'.

3. Change **Open Tickets for new alarms automatically** to Yes.
4. In **Automatic ticket generation default in-charge user/entity**, select the user to whom the ticket will be assigned.
5. If you want to receive emails when a ticket is updated, change **Send email notification** to Yes. USM Appliance sends a notification five minutes after each update to the ticket.
6. In **Open tickets reminder**, you can configure USM Appliance to send a reminder if a ticket has been opened but not updated for a number of days. The default is 15 days.

 **Note:** No email is sent at the opening of the ticket.

To customize vulnerability scan automatic ticket settings

1. Go to **Configuration > Administration > Main**.
2. Expand **Vulnerability Scanner**.
3. Select the ticket threshold for when new tickets are generated in the **Vulnerability Ticket Threshold** drop-down.

Create a Ticket Manually While Investigating an Alarm

To open a ticket manually

1. Go to **Analysis > Alarms > List View** (or **Group View**) and click on the desired alarm.
2. Click **View Details**.
3. From the Alarms Detail page, click **Actions > Create Ticket**.
4. Assign a priority to the ticket and assign it to an administrative user.
5. Click **Save**.



Note: You can also open a remediation ticket from the **Security Events (SIEM) Events** list, using the same steps.

Create a Ticket Independent from an Alarm

To open a ticket manually from the Tickets page

1. From **Analysis > Tickets**, select the type of ticket you want to open and click **Create**.

SIMPLE FILTERS [SWITCH TO ADVANCED]

Class	Type	Search text	Assignee	Status	Priority					
ALL	ALL			Open	ALL	ACTIONS				
<input type="checkbox"/>	TICKET	TITLE	PRIORITY	CREATED	LIFE TIME	ASSIGNEE	SUBMITTER	TYPE	STATUS	LABELS
<input type="checkbox"/>	ALA02	New Alarm incident	4	2017-10-02 16:40:03	7 Days 04:03	dfield	dfield	Anomalies	Open	
<input type="checkbox"/>	EVE01	Welcome to AlienVault	2	2017-09-26 04:52:07	13 Days 15:51	Admin		Generic	Open	

Open a new ticket manually: Alarm **CREATE**

- Generic
- ✓ Alarm
- Event
- Vulnerability
- Anomalies
- Mac
- OS
- Services



Note: You can create a custom ticket type by clicking on the pencil icon in the Type column.

2. Fill in the fields of the dialog box with relevant information to this ticket, including to whom to assign the ticket.



Note: Only tickets created from an alarm contain pre-filled fields.

3. Click **Save**.

Search and Close Tickets

USM Appliance lets you search for a particular ticket and use various search criteria to help you refine your results. The tickets from the search can be reviewed and closed individually, or all together as a batch.

Search for Tickets

To filter the displayed tickets

1. Go to **Analysis > Tickets** and select **Simple Filters** or **Advanced Filters**.

Simple Filters is the default search view, while the Advanced search allows for more filters for fine-tuning the results.

2. Input the filter values and then click **Search**.

The Priority filter has the following relationship with the priority value in the tickets:

Priority in the Filter	Priority in the Ticket
Low	1-4
Medium	5-7
High	8-10

Close or Delete Tickets

To close or delete tickets

1. Go to **Analysis > Tickets**, and do a search to filter for the tickets you want to find.
2. Click the checkbox next to the tickets you want to select for closing or deletion. To select all of the tickets from your search, click the top checkbox in the header.
3. Click **Actions** and then click either **Close** or **Delete**.

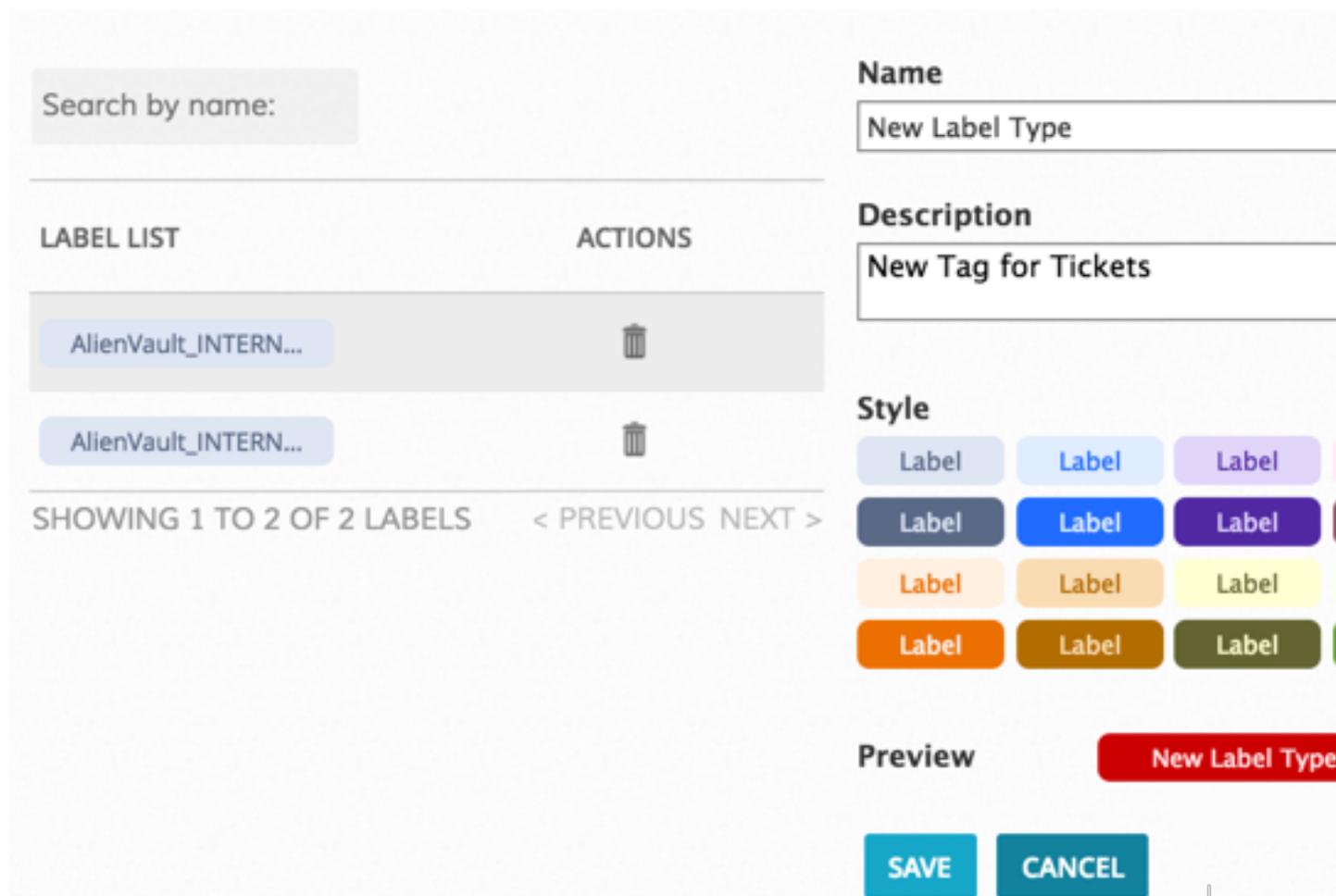
Ticket Labels

Tickets tags can be used as a quick method of identifying and filtering tickets. USM Appliance comes configured with two default tags that can be assigned to tickets: AlienVault_Internal_Pending and AlienVault_Internal_False_Positive. Tickets generated by the vulnerability scans are automatically assigned the Alienvault_Internal_Pending tag to indicate that the vulnerability hasn't been investigated yet.

To create new label types:

1. Go to **Analysis > Tickets**.
2. Click the  icon and click **Manage Labels**.
3. Give the new label a name and description and choose a color for the label.
4. Click **Save**.

MANAGE LABELS



The screenshot displays the 'MANAGE LABELS' interface. On the left, there is a search bar labeled 'Search by name:' and a table with two columns: 'LABEL LIST' and 'ACTIONS'. The table contains two entries, both labeled 'AlienVault_INTERN...', each with a trash icon in the 'ACTIONS' column. Below the table, it says 'SHOWING 1 TO 2 OF 2 LABELS' and '< PREVIOUS NEXT >'. On the right, there is a form to create a new label. It has a 'Name' field with 'New Label Type', a 'Description' field with 'New Tag for Tickets', and a 'Style' section with a grid of 12 color swatches. Below the style section is a 'Preview' area showing a red label with the text 'New Label Type'. At the bottom right, there are 'SAVE' and 'CANCEL' buttons.

Edit a Ticket

On **Analysis > Tickets**, you can search for the ticket you want to update, and then select the ticket by clicking its ticket number or its title within the list. A new page displays that allows you to view the ticket's details and edit the ticket, delete it, or add a comment to it.

TICKET ID	TICKET	STATUS	PRIORITY	KNOWLEDGE DB	ACTION
ALA02	<p>Name: New Alarm incident</p> <p>Class: Alarm</p> <p>Type: Anomalies</p> <p>Created: 2017-10-02 16:40:03 (7 Days 02:36)</p> <p>Last Update: 6 Days 22:36</p> <p>In charge: dfield</p> <p>Submitter: dfield</p> <p>Extra: n/a</p> <p>Source Ips:</p> <p>Source Ports:</p> <p>Dest Ips:</p> <p>Dest Ports:</p>	Open	4	DOCUMENTS	  
				No linked documents	
				 LINK EXISTING DOCUMENT	
				 NEW DOCUMENT	
				Admin (No email) 	SUBSCRIBE UNSUBSCRIBE

To make changes to a ticket

1. Within a ticket, you can make the following changes:

- **Edit**

Use the  icon under Action at the upper right-hand corner.

Changes can consist of the following:

- Status (open, closed, assigned, studying, waiting, testing).
- Priority (low is 1 and 10 is high).
- Transfer the ticket to another administrative user.

- **Add a comment**

For example, you can describe actions taken on the ticket.

- **Delete**

Use the  icon under Action at the upper right-hand corner or click **Delete Ticket** farther down on the page.

- **Subscribe or Unsubscribe**

Follow any updates to this ticket by selecting your name from the list box and clicking **Subscribe** or **Unsubscribe**.

- **Link Existing Document**

Link an existing file with relevance to the ticket.

- **New Document**

Create a new file to go with the ticket.

2. When finished, click **Save Ticket**.

After USM Appliance saves the changes, you see each new entry displayed in the lower half of the Tickets page.

4. If you delete a comment or make any other changes, click **Save Ticket** again.

Correlation and Cross-Correlation

Event Correlation is a key process performed by the AlienVaultUSM Appliance systems. And cross-correlation is a special type of correlation, which correlates vulnerability with network intrusion events.

This section covers the following subtopics:

Event Correlation	228
Correlation Contexts	230
Correlation Directives	230
Tutorial: Create a New Directive to Detect DoS Attack	242
Tutorial: Modifying a Built-In Directive	249
Cross-Correlation	253

Event Correlation

Event Correlation is a key process performed by the AlienVault USM Appliance systems.

What Is Correlation?

Correlation is a process performed by the correlation engine on the AlienVault USM Appliance Server. It identifies potential security threats by detecting behavior patterns across different types of assets, which produce disparate yet related events. Correlation links different events, turning data into more useful information.

The logs received and processed by USM Appliance carry important information such as what your users are doing, what data is being accessed, how your system and network are performing, and if there are any security threats or attacks taking place. However, reading raw logs has the following disadvantages

- Logs vary from system to system or even from version to version on the same system
- Logs have limited perspective, because each system sees events from its own perspective
- Logs are static, fixed points in time, without the full context or sequence of related events

The correlation process on USM Appliance provides answers to these challenges, putting the events into full context. For example, a network firewall sees packets and network sessions, while an application sees users, data, and requests. While different systems report logs of similar activities, the way in which they articulate these activities is quite different. With the help of correlation directives, USM Appliance can correlate the two types of events, generating an alarm if a threat exists.

Event correlation enables security analysts and incident responders to:

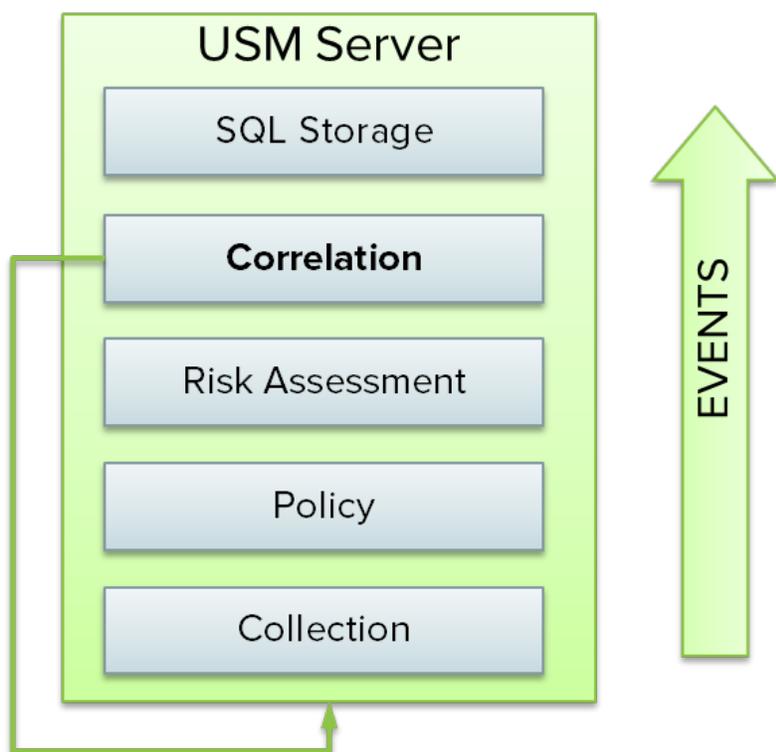
- Make informed decisions on how to respond to security threats
- Validate effectiveness of existing security controls
- Measure and report compliance
- Detect policy violations

How Does Correlation Work?

Correlation typically associates multiple events, of the same or different event types, from the same data source.

After the USM Appliance Server receives normalized events from a USM Appliance Sensor, it evaluates the events against the policies, performs the risk assessment, and then does correlation. The correlation engine applies correlation rules to the events, generating new events, if pertinent, with higher priority and/or reliability values. In such cases, USM Appliance injects the event into the USM Appliance Server as a new event, so that it goes through the same processing sequence again.

An event is required to trigger the subsequent steps in a directive correlation. In instances when an event is not received, the directive will close with a timeout, and no new alarms will be created beyond the ones previously initiated by the directive.



Event processing on the USM Appliance Server

Correlation directives, which contain one or more correlation rules, determine whether or not to connect certain events. The following figure shows a high-level example of a correlation directive. This directive detects brute force authentication events by connecting two types of events, *Failed Logins* and *Successful Login*. Based on the number of occurrences of individual events, the correlation engine can conclude that the event represents a case of an administrator mistyping a password (one failed login attempt followed by a successful login), a successful brute force attack with low reliability (10 failed login attempts followed by a successful login), or a successful brute force attack with high reliability (100,000 failed login attempts followed by a successful login). All these events need to come from the same IP

address and go to the same IP address, in order for the directive event to be created. The correlation engine can also take into account the reputation of source and destination IP addresses, and match specific rules only if an event is coming from, or destined to, a host with a bad reputation.

Correlation Contexts

USM Appliance uses Correlation Contexts to allow overlapping networks. A USM Appliance Server can handle overlapping networks when they are connected to different USM Appliance Sensors. A common use case would be two branches of the same company using the same private addresses, but obviously belonging to different networks. In this case, you can deploy different USM Appliance Sensors to monitor different networks, and use Contexts to differentiate events coming from overlapping IP addresses by assigning a unique Context to each USM Appliance Sensor. You can then create policies or run reports on individual contexts.



Note: Directives do not support contextual filtering as they are processed at the server level. However, you can create correlation rules based on a specific sensor, achieving a similar effect.

When a USM Appliance Server or USM Appliance All-in-One detects that a new USM Appliance Sensor tries to connect, on the **Configuration > Deployment > Sensors** page, it posts the following question:

"Does this sensor monitor a network already monitored by another sensor?"

If selecting "yes", you need to select a sensor that monitors the same network; thus the two sensors share the same Context.

If selecting "no", USM Appliance creates a new Context for this new sensor, allowing for network overlapping.

Correlation Directives

USM Appliance provides over 4,500 built-in directives and adds more every week through the AT&T Alien Labs™ Threat Intelligence Update. The directives are grouped into different categories.

USM Appliance correlation directive categories

Category Name	Explanation	Example
User Contributed	A placeholder for user created and/or modified directives. By default, this category is empty.	
AlienVault Attacks	Directives to detect various attacks against vulnerable services and applications.	AV Attacks, Successful OpenSSL HeartBeat attack
AlienVault BruteForce	Directives to detect brute force attacks on services that require authentication.	AV Bruteforce attack, SSH authentication attack against DST_IP (destination IP)
AlienVault DoS	Directives that detect Denial of Service (DoS) attacks on different applications and services.	AV Service attack, successful denial of service against IIS web server on DST_IP (MS07-041)
AlienVault Malware	Directives to detect malware.	AV Malware, botnet Koobface activity detected on SRC_IP (source IP)
AlienVault Misc	Directives to detect activities that do not fall into any other category.	AV Misc, suspicious executable download from a dynamic domain on SRC_IP
AlienVault Network	Directives detect network related anomalies and attacks.	AV Network attack, too many dropped inbound packets from DST_IP
AlienVault Policy	Directives to detect policy violations.	AV Policy violation, vulnerable Java version detected on SRC_IP
AlienVault Scada	Directives to detect attacks on industrial supervisory control and data acquisition (SCADA) systems.	AV SCADA attack, Modbus scanning or fingerprinting against DST_IP
AlienVault Scan	Directives to detect scanning activities.	AV Network scan, Nmap scan against DST_IP

USM Appliance provides a web interface, **Configuration > Threat Intelligence > Directives**, for you to examine, modify, or create new correlation directives.

Correlation Directives Found 3,419 directives in the system

New Directive |
 Test Directives |
 Reload Directives |
 Search a directive name: **SEARCH**

User Contributed Custom directives

- ▶ **AlienVault Attacks** [871 directives]
- ▶ **AlienVault BruteForce** [115 directives]
- ▶ **AlienVault DoS** [12 directives]
- ▶ **AlienVault Malware** [2149 directives]
- ▶ **AlienVault Misc** [17 directives] Built-in directives
- ▶ **AlienVault Network** [30 directives]
- ▶ **AlienVault Policy** [140 directives]
- ▶ **AlienVault Scada** [12 directives]
- ▶ **AlienVault Scan** [73 directives]

To display a directive

1. Click the black triangle to the left of the category name.
2. Click the black triangle to the left of the directive.

Each directive consists of the following

- [Global properties](#)
- [One or more rule\(s\)](#)
- [Directive Info](#)
- (Optional) [Knowledge Base article\(s\)](#)



AlienVault OSSIM Limitations: In the AlienVault OSSIM environment, the following directives are inactive

- AlienVault DoS
- AlienVault Network
- Alienvault Scada

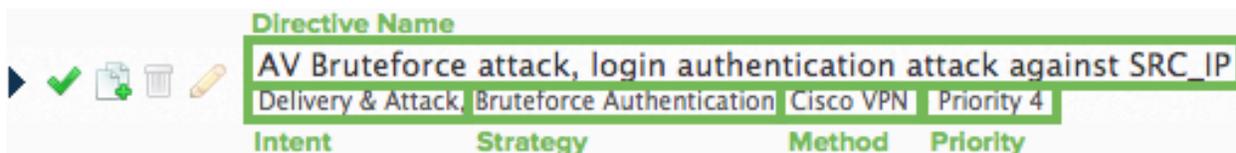
Global Properties

Each correlation directive has the following global properties

Global properties for correlation directives

Property	Description
ID	A unique identifier for the directive. It becomes the Event Type ID when a directive event is created. Note: The ID of a directive is not displayed in the web interface.
Name	A meaningful name for the directive. It becomes the name of the directive event or the alarm.
Intent, Strategy, Method	Describe what the correlation directive tries to detect. These properties help categorize directive events according to the AlienVault USM Appliance Taxonomy.
Priority	Defines the impact of the detected attack. USM Appliance uses it in the risk calculation of a directive event. All events generated by the directive have their priority set to the priority value of the directive.

The following screen shot gives you an example of the global properties of a directive:



Correlation Rules

A correlation rule defines a condition to match incoming events. Refer to [How Does Correlation Work?](#) for details. The table below summarizes the attributes used in the rules.

Correlation Rule Attributes

Attribute	Attribute Type	Description
Name	String	Name of the rule. Each rule has its own name within the directive, and they can be the same.
Reliability	Number	The reliability value that the rule assigns to the event. It ranges from 0 to 10.
Timeout	Number	<p>The waiting time (in seconds) before the rule expires and the correlation process using that rule stops. The default value is 300 seconds.</p> <p>The Timeout value for the first rule is None, indicating that the rule does not expire. None is not a valid entry for subsequent rules in the directive.</p>
Occurrence	Number	Number of times an event has to occur in order for the rule to match.
From	String	<p>Source IP and port(s) that the rule tries to match.</p> <p>In addition to a specific host name or IP, you may also see variables used in this field, such as ANY, HOME_NET (defined in Environment > Assets & Groups > Networks), SRC_IP, SRC_PORT, DST_IP, or DST_PORT.</p>
To	String	<p>Destination IP and port(s) that the rule tries to match.</p> <p>In addition to a specific host name or IP, you may also see variables used in this field, such as ANY, HOME_NET (defined in Environment > Assets & Groups > Networks), SRC_IP, SRC_PORT, DST_IP, or DST_PORT.</p>
Data Source	String	Data source (or plugin) name and ID that the rule tries to match.
Event Type	String	<p>Event type ID (SID) that the rule tries to match.</p> <p>When there are multiple SIDs specified, the rule tries to match any of them.</p>
Sensor	String	The USM Appliance Sensor that sends the events.
Protocol	String	The protocol specified in an event. Accepted values are ANY, TCP, UDP, and ICMP.

Correlation Rule Attributes (Continued)

Attribute	Attribute Type	Description
Sticky Dif	List	Attributes in directive rules are sticky by default. This means that when a new event arrives at the correlation engine, USM Appliance correlates it with the previous event if the event attributes (such as IP address or port number) are the same. However, attributes in a directive can also be sticky different. When set, an arriving event needs to have a different value than the previous one in order to be correlated. For example, in port scanning attacks, if you set the destination port as sticky different, only events with different destination ports are correlated for the directive. Accepted values for this attribute are None, Plugin_sid, SRC_IP, DST_IP, SRC_Port, DST_Port, Protocol, and Sensor.
Username	String	The username specified in the event.
Pass	String	The password specified in the event.
Userdata1-Userdata9	String	The user data fields specified in the event.

By default, USM Appliance only displays the attributes up to Event Type. To see the additional attributes, click the **More** button. The majority of the built-in directives do not use these attributes.

AV Attacks, Possible DDoS using SQL servers
Delivery & Attack, Denial of Service - Resource exhaustion, Reflection using SQL servers - Priority 5

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
MC-SQLR Response	1	None	1	!HOME_NET	HOME_NET	AlienVault NIDS (1001)	SIDs: 2020306	More
MC-SQLR Response	5	600	5	ANY	1:DST_IP	AlienVault NIDS (1001)	SIDs: 2020306	More
MC-SQLR Response	8	86400	10000	ANY	1:DST_IP	AlienVault NIDS (1001)	SIDs: 2020306	More

DIRECTIVE

SENSOR	PROTOCOL	STICKY DIF	FILENAME	USERNAME	PASS	USERDATA1	USERDATA2	USERDATA3	USERDATA4	USERDATA5	USERDATA6	USERDATA7	USERDATA8	USERDATA9
ANY	ANY	SRC_IP												

Delivery & Attack, Denial of Service - Resource exhaustion, SlowLoris - Priority 5

Note: To examine which event the SID represents, click the data source name, and then search for the SID in the resulting page. The SID does not respond even though it appears like a link.

To change which attributes to display

1. Click the [...] next to the **Event Type** column.

AV Attacks, Possible DDoS using SQL servers
Delivery & Attack, Denial of Service - Resource exhaustion, Reflection using SQL servers - Priority 5

RULES								[...]
NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	
▼ MC-SQLR Response	1	None	1	!HOME_NET	HOME_NET	AlienVault NIDS (1001)	SIDs: 2020306	► More
▼ MC-SQLR Response	5	600	5	ANY	1:DST_IP	AlienVault NIDS (1001)	SIDs: 2020306	► More
MC-SQLR Response	8	86400	10000	ANY	1:DST_IP	AlienVault NIDS (1001)	SIDs: 2020306	► More

► DIRECTIVE INFO

The **Customize Columns** window opens.

2. Select which attributes you want display in a rule.

CUSTOMIZE COLUMNS

Select the columns to show in the rules, the rest will be in the 'More' tab

8 items selected	Remove all	
Name	—	Sensor
Reliability	—	Protocol
Timeout	—	Sticky Dif
Occurrence	—	Username
From	—	Pass
To	—	Userdata1
Data Source	—	Userdata2
Event Type	—	Userdata3
		Userdata4
		Userdata5
		Userdata6

SAVE

CANCEL

3. Click **Save**.

Indentation of Rules

When a correlation directive contains multiple rules, the indentation of the rules reveals the relationship between the rules. Indented rules have an AND relationship while parallel rules have an OR relationship.

For example, the screenshot below shows one of the built-in directives, **AV Network attack, too many dropped inbound packets from DST_IP**, which detects network attacks by observing dropped packets from any source IP address to a specific destination IP address on the Cisco PIX firewall. This directive has three correlation levels (denoted by the black triangles) and four rules (all named **Firewall dropped packets**).

AV Network attack, too many dropped inbound packets from DST_IP Environmental Awareness, Network Anomaly, Too many dropped Inbound packets - Priority 2								
RULES								
	NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE
	Firewall dropped packet	2	None	1	ANY	ANY	cisco-pix (1514)	SIDs: 106011
AND	Firewall dropped packets	4	10	3	ANY	1:DST_IP	cisco-pix (1514)	SIDs: 106011
AND	Firewall dropped packets	6	20	5	ANY	1:DST_IP	cisco-pix (1514)	SIDs: 106011
OR	Firewall dropped packets	8	30	10	ANY	1:DST_IP	cisco-pix (1514)	SIDs: 106011

The first rule is matched when the cisco-pix plugin identifies a "PIX:Deny inbound (No xlate) string" (SID 106011) event. AND, if the second rule also matches, 3 more such events occur within 10 seconds toward the same destination, the reliability of the directive event increases to 4. AND, if the third rule also matches, 5 more such events occur within 20 seconds toward the same destination, the reliability increases to 6. OR, if the last rule matches, 10 more such events occurred within 30 seconds toward the same destination, the reliability of the directive event increases to 8.

Using Negation and Commas

You can use negation (inserting an exclamation point before an item) to exclude items in a rule. Commas can be used to separate items when creating lists. Specific considerations must be made when using commas and exclamation points together in lists. When using commas to separate multiple elements in a list, the list must consist of exclusively non-negated items, or only negated items, and not a combination of both. Because a negation implies anything which is not the item being negated, the inclusion of non-negated items in the same list will create a contradictory logic for the scope of the list. For example, using a negation such as `plugin_sid="5901, !5902"` states that the rule will occur when matched with the plugin signature ID of 5901, while simultaneously stating that everything that doesn't match plugin signature ID 5902 should be used to match the rule, creating a contradiction in what will trigger the event. This logic also extends to subsequent rules in the directive.

Using Attribute Values from the Previous Rule

When there are multiple rules in a directive, subsequent rules often use the same value set in the previous rule. In the example above, the "1:DST_IP" notation in the TO attribute means to keep using the same destination IP selected in the first rule, to look for attacks against the same host. You can manually select the destination IP again, or you can use the option **From a parent rule: Destination IP from level 1**:

DESTINATION HOST/NETWORK

From a parent rule: Destination IP from level 1

DESTINATION PORT(S)

· Use comma to specify several ports.
 · Can be negated using '!'

From a parent rule: ANY

▶ Reputation options

You will find this option available when setting the Source, Source Port, Destination, Destination Port, Event Type (must select the data source first), and Sensor attributes. In addition, when editing **String** type attributes (see [Correlation Rule Attributes](#)), you can use the same <rule number>:<attribute name> notation. For example, "2:USERNAME" would mean to use the same user name chosen in the second rule.

Directive Information

The **Directive Info** (directive information) section displays information used by USM Appliance for compliance mapping and/or reports. It also lists the alarms this directive has triggered, if any.

The first column on the left lists some additional information (called properties) about the directive, such as what kind of an attack the directive detects.

In the example below, the directive detects too many packets being dropped, which classifies it as a **Network Anomaly**.



Note: **IMP** is short for IMPact; **QOS** means Quality of Service; and **Infleak** is short for Information leak.

These properties, when set, are used in the *B & C – Trends* section of the Business and Compliance report, one of the built-in reports in the USM Appliance.

▼ AV Network attack, too many dropped inbound packets from DST_IP
Environmental Awareness, Network Anomaly, Too many dropped inbound packets

▼ RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
Firewall dropped packet	2	None	1	ANY	ANY	cisco-pix (1514)	SIDs: 106011	► More
▼ Firewall dropped packets	4	10	3	ANY	1:DST_IP	cisco-pix (1514)	SIDs: 106011	► More
▼ Firewall dropped packets	6	20	5	ANY	1:DST_IP	cisco-pix (1514)	SIDs: 106011	► More
Firewall dropped packets	8	30	10	ANY	1:DST_IP	cisco-pix (1514)	SIDs: 106011	► More

▼ DIRECTIVE INFO

PROPERTIES	ISO27001	PCI DSS 2.0	PCI DSS 3.0	ALARMS
Targeted				
Approach				
Exploration				
Penetration				
General Malware				
IMP QOS				
IMP Infleak				
IMP Lawful				
IMP Image				
IMP Financial				
IMP Infleak				
Availability				
Integrity				
Confidentiality				
Net Anomaly				

EDIT REMOVE

► KNOWLEDGE DB

You can change the default values of these properties using the **Edit** button. You can also clear all properties by clicking **Remove**.

The next three columns, **ISO 27001**, **PCI DSS 2.0**, and **PCI DSS 3.0**, display compliance information about the directive, if mapped. This information is then used in the USM Appliance reports.



Note: You cannot change the compliance mapping in a built-in directive.

The following figure displays an example of a directive that has PCI DSS compliance information:

AV Client side attack, malicious host successful exploited Adobe Reader against DST_IP (CVE-2009-0658)
Exploitation & Installation, Client Side Exploit - Known Vulnerability, Adobe Reader - CVE-2009-0658

▼ RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
▼ Nginx web server detected	0	None	1	!HOME_NET	ANY	snort (1001)	SIDs: 2008064 2008065	► More
Adobe PDF JBIG2	6	60	1	1:SRC_IP	1:DST_IP	snort (1001)	SIDs: 2800429	► More

▼ DIRECTIVE INFO

PROPERTIES	ISO27001	PCI DSS 2.0	PCI DSS 3.0	ALARMS
Targeted ● Approach ● Exploration ● Penetration ● General Malware ● IMP QOS ● IMP Infleak ● IMP Lawful ● IMP Image ● IMP Financial ● IMP Infleak ● Availability ● Integrity ● Confidentiality ● Net Anomaly ● EDIT REMOVE	No ISO27001 found	R.6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	R.6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	No Alarms found

► KNOWLEDGE DB

The last column displays alarms that this directive has triggered.

When such alarms exist, the **Alarms** column displays their name, risk, and status. The directive in the example below triggered an alarm with a risk of 3. The status of the alarm is open, as indicated by the open lock icon.

AV Network scan, Nmap scan against DST_IP
Reconnaissance & Probing, Portscan, Nmap

▼ RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
Network scan with Nmap detected	8	None	1	!HOME_NET	HOME_NET	snort (1001)	SIDs: 2000544 2000543 2000540 2000538 2009584 2000536 2009583 2009582 2000537 2009358 2009359 2101228 2100628 2100629 2000545 2000546 2013778	► More
Network scan with Nmap detected	8	3600	1	1:SRC_IP	HOME_NET	snort (1001)	SIDs: 2000544 2000543 2000540 2000538 2009584 2000536 2009583 2009582 2000537 2009358 2009359 2101228 2100628 2100629 2000545 2000546 2013778	► More
Network scan with Nmap detected	8	3600	50000	1:SRC_IP	HOME_NET	snort (1001)	SIDs: 2000544 2000543 2000540 2000538 2009584 2000536 2009583 2009582 2000537 2009358 2009359 2101228 2100628 2100629 2000545 2000546 2013778	► More

▼ DIRECTIVE INFO

PROPERTIES	ISO27001	PCI DSS 2.0	PCI DSS 3.0	ALARMS						
Targeted Approach Exploration Penetration General Malware IMP QOS IMP Inleak IMP Lawful IMP Image IMP Financial IMP Inleak Availability Integrity Confidentiality Net Anomaly	No ISO27001 found	No PCI DSS 2.0 found	No PCI DSS 3.0 found	<table border="1"> <thead> <tr> <th>NAME</th> <th>RISK</th> <th>STATUS</th> </tr> </thead> <tbody> <tr> <td>AV Network scan, Nmap scan against DST_IP</td> <td>3</td> <td></td> </tr> </tbody> </table>	NAME	RISK	STATUS	AV Network scan, Nmap scan against DST_IP	3	
NAME	RISK	STATUS								
AV Network scan, Nmap scan against DST_IP	3									

► KNOWLEDGE DB

Knowledge DB

Some built-in correlation directives also include a link that points to a document in the AlienVault Knowledge Base (**Configuration > Threat Intelligence > Knowledge Base**). The Knowledge Base contains vendor provided information on a vulnerability or knowledge from the information security community. It provides suggestions to security analysts and incident response teams on where to look for information about an activity or an attack.

To read the document linked to the directive

- Expand the **Knowledge DB** option, and then click the title of the document.

For example, the following directive, which detects an exploit in Internet Explorer, includes a Knowledge Base document that describes the exploit and where to find more information about the exploit.





AV Client side attack, attack detected against DST_IP (MS06-057)
 Exploitation & Installation, Client Side Exploit - Known Vulnerability, Microsoft Internet Explorer - CVE-2006-3730

▼ RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
MSIE WebViewFolderIcon setSlice	0	None	1	!HOME_NET	ANY	snort (1001)	SIDs: 2003110 8419	► More
Executable download detected	8	40	1	!HOME_NET	1:DST_IP	snort (1001)	SIDs: 15306 13797	► More
Suspicious executable download detected	10	40	1	!HOME_NET	1:DST_IP	snort (1001)	SIDs: Expand / Collapse 2805352 2805353 2008547 2002773 2009034 2009035 16435 16436 2015752 2014819	► More

► DIRECTIVE INFO

▼ KNOWLEDGE DB

KDB

DATE	TITLE
2012-01-01	AV Client side attack, attack detected against DST_IP (MS06-057)

SHOWING 1 TO 1 OF 1 ENTRIES FIRST PREVIOUS 1 NEXT LAST

Tutorial: Create a New Directive to Detect DoS Attack

Sometimes, you may find that none of the built-in directives work in your environment because they do not have the correct conditions defined. In this case, you can create a new directive from scratch. Let's see how it works by going through an example.

In this example, we create a custom directive to detect a Denial of Service (DoS) attack that seeks to exhaust a service running on TCP port 139 on a specific server. Many connections from a single host (possibly with bad reputation) to the destination server on port 139 may indicate such an attack. We can check firewall events for connections to the server and trigger an alarm after the correlation engine detects that the number of connections is dangerously high.

The following diagram shows the three correlation levels we plan to use in the directive. The three correlation rules check for the number of connections to the server using a detector plugin. Every time a rule in the correlation directive matches an event, the reliability of the directive event increases, thus increasing the risk of the event.



Correlation levels used by the sample directive

Follow the tasks below to create this directive.

Task 1: Create a New Directive Named "DoS Attack at NetBIOS"

To create a new directive

1. Go to **Configuration > Threat Intelligence**, and then click **Directives**.
2. Click **New Directive**.

A pop-up window appears displaying the global properties of the directive.

3. Fill out the form as below
 - In **Name for the directive**, Type "DoS Attack at NetBIOS".
 - In **Intent** select "Delivery & Attack".
 - In **Strategy** select "Denial of Service – Resource exhaustion".
 - In **Method**, type "Attack".
 - Leave the **Priority** at the default value, which is **3**.

NEW DIRECTIVE

NAME FOR THE DIRECTIVE

DoS on NetBIOS

TAXONOMY

Intent: Delivery & Attack

Strategy: Denial of Service - Resource e

Method: Attack

PRIORITY

0

1

2

3

4

5

CANCEL NEXT

4. Click **Next**.

The **New Directive** window displays.

Task 2: Add a Level 1 Rule to Detect the Event

This task adds a level 1 rule for the directive created in Task 1. In this rule, we try to match one Cisco ASA Access Permitted event on a particular server on port 139.

To add a level 1 rule

1. In **Name for the Rule**, type "Established connections", and then click **Next**.
2. In **Rule name > Plugin**, type "cisco-asa" in the search box, and then click **Cisco-ASA**.
3. In **Rule name > Plugin > Event Type**,

- a. Type "permitted" in the search box.

A list of ASA event types with the word "permitted" in their description displays in the right column.

- b. To select the event types identified, click the plus (+) sign to the right of each event type or click **Add all**.

NEW DIRECTIVE

Rule name > Plugin > Event Type

Choose between Event Sub-Types Selection or Taxonomy

Event Sub-Types Taxonomy

PLUGIN SIGNATURES

0 items selected Remove all permitted Add all

106102 - ASA: A packet was either permitted or denied by an acces...	+
710002 - ASA: Access Permitted	+
717015 - ASA: An IPsec connection caused a CRL that is larger than...	+

Empty selection means ANY signature

CANCEL BACK NEXT

- c. Click **Next**.

4. In **Rule name > Plugin > Event Type > Network**,

- a. Select your server from the Assets list under **Destination Host / Network**.

The server appears in **Destination**.



Note: Leave **Source Host / Network** and **Source Port(s)** empty, which means *any* asset.

- b. In **Destination Port(s)**, type "139".

- c. (Optional) To specify IP reputation parameters, click the green triangle next to **Reputation options**, change No to Yes, and then select the Min Priority and Min Reliability values.

Note: For details on IP reputation, see [OTX IP Reputation](#).

- d. Click **Next**.

5. In **Rule name > Plugin > Event Type > Network > Reliability**, click **1**.

Note: We choose a low reliability value because typically the level 1 rule detects that a certain event occurs, but it is not necessary to generate an alarm.

6. Click **Finish**.

The **New Directive** window closes.

Task 3: Add a Level 2 Rule to Detect the Same Event with 100 Occurrences

In this task, we try to match the same events selected in Task 2. We want to use the

- same event types
- same source and destination IP addresses
- same destination port

But we want to detect 100 such events instead of 1.

To add a level 2 rule

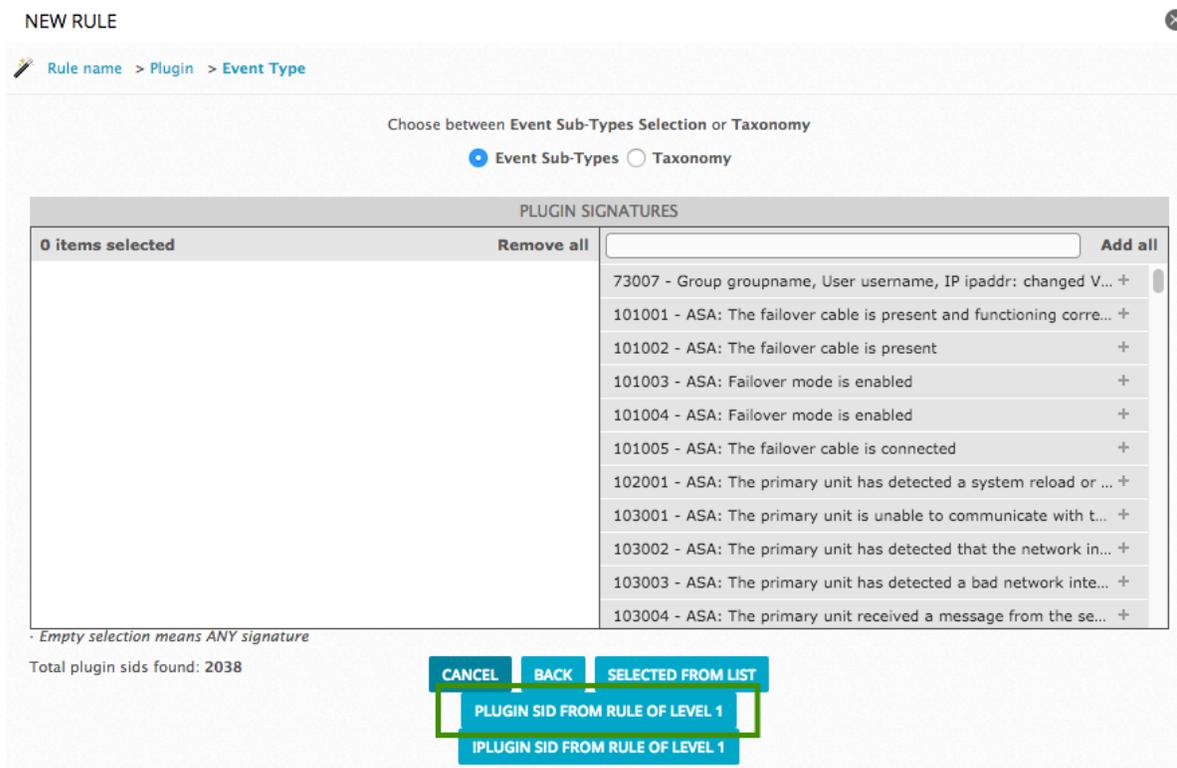
1. Click the green plus (+) sign at the right side of the first rule, under the **Action** heading.



The **New Rule** window displays.

2. In **Name for the Rule**, type "Established connections", and then click **Next**.
3. In **Rule name > Plugin**, type "cisco-asa" in the search box, and then click **Cisco-ASA**.
4. In **Rule name > Plugin > Event Type**, click **Plugin SID from rule of Level 1**.

This selects the same event types as in the level 1 rule.



5. In **Rule name > Plugin > Event Type > Network**,

- a. In **Source Host / Network**, under **From a parent rule**, select "Source IP from level 1".

This selects the same source IP address as in the level 1 rule.

- b. Leave the **Source Ports** empty.

- c. In **Destination Host / Network**, under **From a parent rule**, select "Destination IP from level 1".

This selects the same destination IP address as in the level 1 rule.

- d. In **Destination Port(s)**, under **From a parent rule**, select "Destination Port from level 1".

This selects the same destination port as in the level 1 rule.

NEW RULE

Rule name > Plugin > Event Type > Network

NETWORK

· Empty selection means ANY asset

SOURCE HOST/NETWORK

DESTINATION HOST/NETWORK

From a parent rule: Source IP from level 1

From a parent rule: Destination IP from level 1

SOURCE PORT(S)

DESTINATION PORT(S)

· Use comma to specify several ports
· Can be negated using '!'

From a parent rule:

From a parent rule: Destination Port from level 1

▶ Reputation options

▶ Reputation options

CANCEL BACK NEXT

6. In **Rule name > Plugin > Event Type > Network > Reliability**, click **+2**.

Note: In this step, you can either choose an absolute value (left column) or a relative value (right column). If you select a relative value, as we did, USM Appliance adds the value to the reliability set in the previous rule.

7. Click **Finish**.

The **New Directive** window closes.

8. In the **Timeout** column, click "None" in the second rule, type "30" (seconds), and then click **OK**.
9. In the **Occurrence** column, click "1" in the second rule, type "100", and then click **OK**.



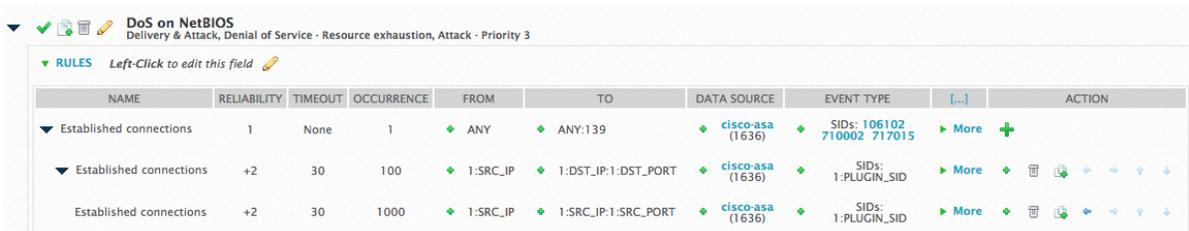
Task 4: Add a Level 3 Rule to Detect the Same Event with 1000 Occurrences

This task is a repeat of Task 3. You can repeat this task as many times as necessary. In this example, we want to add another rule (level 3) to detect the same event as in the previous rule but with 1000 occurrences.

To add the level 3 rule

1. Click the green plus (+) sign at the right side of the second rule, under the **Action** heading. The **New Rule** window displays.
2. Follow step 2 to 7 in Task 3.
3. In the **Occurrence** column, click "1" in the third rule, type "1000", and then click **OK**.

The directive looks similar to this one



Task 5: Reload Directives

To apply all the changes made

1. Click **Reload Directives**. The text displays in red, suggesting an action.
2. Click **Yes** to confirm when prompted.

This step does not restart USM Appliance; it restarts the `ossim-server` process running on USM Appliance.

Tutorial: Modifying a Built-In Directive

USM Appliance comes with over 4,500 built-in directives, written by the researchers in the AT&T Alien Labs™. AlienVault recommends that you learn how these directives work, and then tailor them to your specific needs.

For example, you might want to detect dropped packets going to a single host on a firewall. In the built-in directives, such a directive exists, which detects dropped packets on the Cisco PIX firewall. However, in order to detect dropped packets on a different firewall, for instance, the Fortinet FortiGate firewall, you need to customize the directive.

In this topic, we use this example to show the steps required to modify a built-in directive. It involves the following 4 tasks:

Task 1: Clone an Existing Directive

To clone an existing directive

1. Go to **Configuration > Threat Intelligence**, and then click **Directives**.
2. To find the appropriate directive, type "packets" in the search box.
3. Scroll down on the page to locate the directive titled **AV Network attack, too many dropped inbound packets from DST_IP**.
4. Click the clone icon () to clone the directive.
5. Click **YES** to confirm when prompted.

The cloned directive appears in the **User Contributed** category.

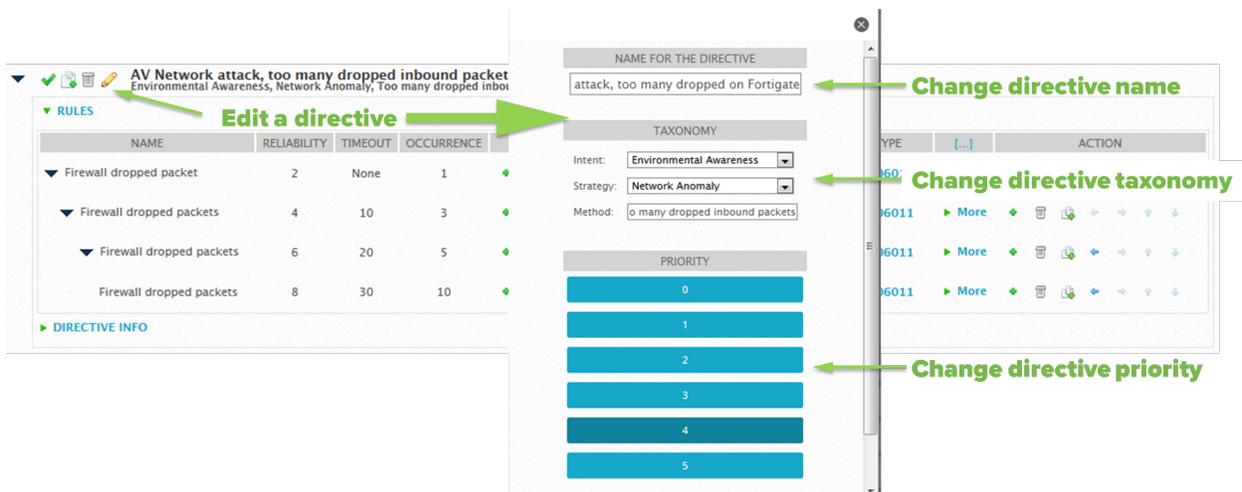
Task 2: Edit the Directive's Global Properties

To edit the cloned directive

1. Click the pencil icon () to the left of the directive.

A pop-up window appears displaying the global properties of the directive.

2. Change the name to "AV Network attack, too many dropped on Fortigate".
3. (Optional) Modify the taxonomy and/or priority of the directive.
4. Click **Save**. You may need to scroll down to reveal the button.



Task 3: Edit the Correlation Rules

Now, you need to edit the correlation rules so that they match the events from the Fortinet FortiGate firewall.

To edit the correlation rules

1. Click the black triangle to the left of the directive to display the correlation rules.
2. In the first rule (first line in the table), under the **Data Source** column, click the green plus (+) sign to the left of **cisco-pix**.

The **Rule Data Source Configuration** window displays.

3. To find the Fortigate plugin, type "fortigate" in the search box.
4. To select that plugin, click **Fortigate**.
5. In Plugin Signatures, to search for the event type(s) that detects dropped packets, type "drop" in the search box.

3 - Fortigate: Drop Forbidden Traffic lists in the right column.

6. To select the event type identified, click the plus (+) sign to the right of the event type, or click **Add all**.

The event type moves to the left column.

7. Click **Finish**.
8. For the remaining rules in the directive, do one of the following to select the same event

type:

- Repeat step 2 to 6, and then click **Selected from List**.
- Repeat step 2 to 4. In Plugin Signatures, click **Plugin SID from rule of level 1**.

The final directive should look like this:

The screenshot shows a configuration page for a directive titled "AV Network attack, too many dropped on Fortigate". Below the title, there is a "RULES" section with a table listing four rules. Each rule has columns for Name, Reliability, Timeout, Occurrence, From, To, Data Source, Event Type, and Action. The rules are all named "Fortigate dropped packet" and have different reliability and timeout values. The first rule has a reliability of 2 and a timeout of None. The second has a reliability of 4 and a timeout of 10. The third has a reliability of 6 and a timeout of 20. The fourth has a reliability of 8 and a timeout of 30. All rules have a "More" link and a green plus sign in the Action column.

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]	ACTION
Fortigate dropped packet	2	None	1	ANY	ANY	fortigate (1554)	SIDs: 3	More	+
Fortigate dropped packet	4	10	3	ANY	1:DST_IP	fortigate (1554)	SIDs: 3	More	+
Fortigate dropped packet	6	20	5	ANY	1:DST_IP	fortigate (1554)	SIDs: 3	More	+
Fortigate dropped packet	8	30	10	ANY	1:DST_IP	fortigate (1554)	SIDs: 3	More	+

You may edit other attributes of the correlation rules, if you want.

To change the Name, Reliability, Timeout, or Occurrence attributes

1. Click the value.
2. Make the changes inline, and then click **OK**.

To change the From or To attributes

1. Click the green plus (+) sign.
2. Make changes in the pop-up window. Notice Source Host and Source Port on the left, Destination Host and Destination Port on the right.
3. Click **Modify**.

To change the Data Source or Event Type attributes

1. Click the green plus (+) sign.
2. Repeat step 2 to step 8 in this task.

Task 4: Reload Directives

To apply all the changes made

1. Click **Reload Directives**. The text displays in red, suggesting an action.
2. Click **Yes** to confirm when prompted.

This step does not restart USM Appliance; it restarts the `ossim-server` process running on USM Appliance.



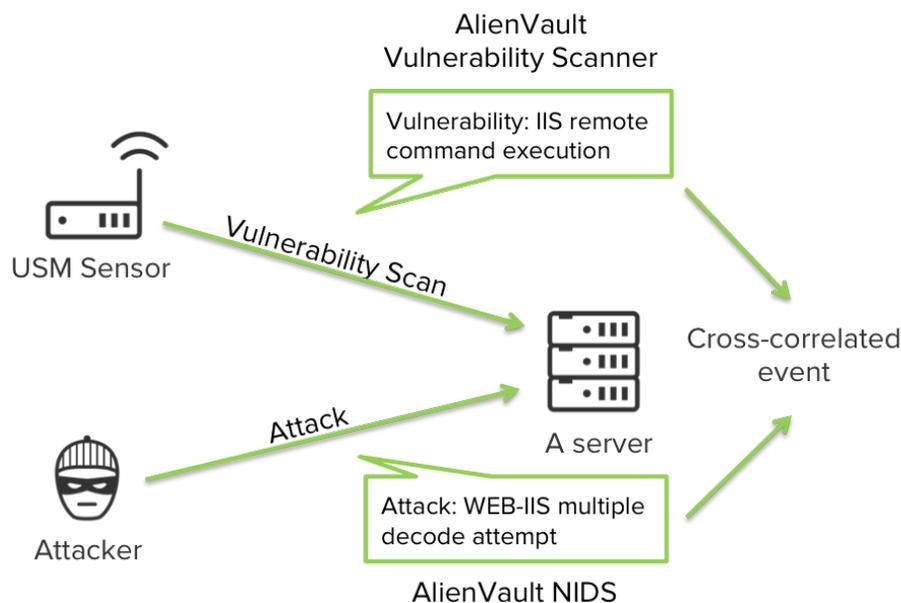
Note: By default, USM Appliance disables the built-in directive automatically after it is cloned. If you want both directives working at the same time, make sure to enable the built-in directive before performing Task 4.

Cross-Correlation

Cross-correlation is a special type of correlation performed by the USM Appliance. The USM Appliance Server uses cross-correlation to modify the reliability of a Network Intrusion Detection System (NIDS) event, which subsequently affects the risk assessment of the event.

USM Appliance only performs cross-correlation on events with destination IP address defined, and the system checks if any vulnerability has been identified on that destination. If the IDS has discovered an attack to an IP address, and a related vulnerability has been found on the same IP, the reliability of the IDS event increases to 10.

The figure below provides an example, where the AlienVault Vulnerability Scanner detects the *IIS remote command execution* vulnerability on a server, and the AlienVault NIDS reports an attack exploiting that vulnerability on the same server.



Cross-Correlation Rules

The correlation engine uses cross-correlation rules to connect NIDS events and vulnerabilities discovered by the AlienVault Vulnerability Scanner.

AlienVault USM Appliance provides a web interface, **Configuration > Threat Intelligence > Cross Correlation** for you to examine, modify, and create cross-correlation rules.

THREAT INTELLIGENCE

POLICY ACTIONS PORTS DIRECTIVES COMPLIANCE MAPPING **CROSS CORRELATION** DATA SOURCE TAXONOMY KNOWLEDGE BASE

SHOW 20 ENTRIES

AlienVault Events		Vulnerabilities	
DATA SOURCE NAME	EVENT TYPE	REF NAME	REF SID NAME
AlienVault NIDS	BACKDOOR Infector 1.6 Server to Client	nessus-detector	nessus: Kuang2 the Virus
AlienVault NIDS	BACKDOOR Infector 1.6 Server to Client	nessus-detector	nessus: scan for LaBrea tarpitted hosts
AlienVault NIDS	BACKDOOR Infector 1.6 Server to Client	nessus-detector	nessus: Apache mod_rootme Backdoor
AlienVault NIDS	BACKDOOR Infector 1.6 Client to Server Connection Request	nessus-detector	nessus: Kuang2 the Virus

NEW MODIFY DELETE SELECTED

At the bottom of the page, you can navigate to the next pages to see more rules. You can also use the search icon to display the search box, and then search by Data Source Name, Event Type, Ref Name, and Ref SID Name.

AlienVault NIDS	FINGER search query	nessus-detector	nessus: Cfingerd 'search' Command Information Disclosure Vulnerability
AlienVault NIDS	FINGER bomb attempt	nessus-detector	nessus: Finger Redirection Remote Denial of Service Vulnerability

Quick Search Data Source Name SEARCH CLEAR

< PREVIOUS NEXT >

To view a cross-correlation rule, do one of the following

- Double-click the rule.
- Highlight the rule and click **Modify**.

For example, the following cross-correlation rule ties an AlienVault NIDS login failed event (for the "sa" account on a Microsoft SQL Server), to when the account has a blank password. The correlated event created in this case would indicate that someone tries to log in to the system using a password, while the system itself has been configured without a password.

INSERT NEW CROSS-CORRELATION RULE

DATA SOURCE NAME	AlienVault NIDS
REFERENCE DATA SOURCE NAME	nessus-detector
EVENT TYPE	"MYSQL client authentication bypass attempt"
REFERENCE SID NAME	nessus: MySQL Authentication bypass through a zero-length passwc

BACK CREATE RULE

AlienVault NIDS Event → Vulnerability

Create a New Cross-Correlation Rule

In this example, we explain how to create a cross-correlation rule to detect a MySQL authentication bypass attempt with an empty password.

To create a new cross-correlation rule

1. Go to **Configuration > Threat Intelligence > Cross Correlation**, and then click **New**.
2. In **Data Source Name**, select "AlienVault NIDS".

USM Appliance loads the Event Type list for AlienVault NIDS.

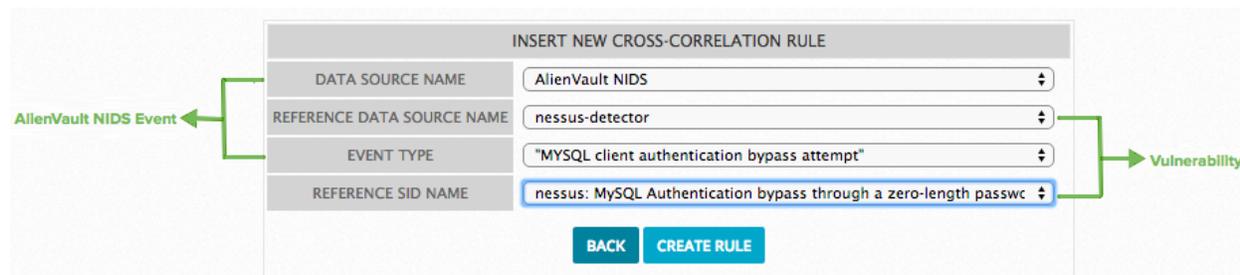
3. In **Reference Data Source Name**, select "nessus-detector", which represents the AlienVault Vulnerability Scanner.

USM Appliance loads the Reference SID Name list for the Vulnerability Scanner.

4. In **Event Type**, select "MYSQL client authentication bypass attempt".

 **Note:** It takes a while for the list to display because it is long.

5. In **Reference SID Name**, select "nessus: MySQL Authentication bypass through a zero-length password".
6. Click **Create Rule**.



INSERT NEW CROSS-CORRELATION RULE	
DATA SOURCE NAME	AlienVault NIDS
REFERENCE DATA SOURCE NAME	nessus-detector
EVENT TYPE	"MYSQL client authentication bypass attempt"
REFERENCE SID NAME	nessus: MySQL Authentication bypass through a zero-length passwc
<input type="button" value="BACK"/> <input type="button" value="CREATE RULE"/>	

Modify a Built-in Cross-Correlation Rule

Similar to correlation directives, you can customize cross-correlation rules as well.

 **Important:** Even though the web interface gives an impression that you can cross-correlate events from any data source with those from any other data source, in fact you can only correlate NIDS events with vulnerabilities detected by the AlienVault Vulnerability Scanner.

To edit an existing cross-correlation rule

1. Highlight the rule you want to edit and click **Modify**.
2. Change any of the four fields as desired.
3. Click **Save Rule**.

Policy Management

This section covers the following subtopics:

Use of Policies in USM Appliance	259
Create or Modify a Policy	268
Policy Order and Grouping	286
Tutorial: Create a Policy to Discard Events	288
Tutorial: Create a Policy to Send Emails Triggered by Events	291
Tutorial: Create a Policy to Send Emails for Account Lockout Events	295

Use of Policies in USM Appliance

USM Appliance uses policies to configure how events are processed. Policies define one or more conditions that are evaluated for each incoming event to determine whether the associated action is triggered. Policies play a critical role in the management of effective incident response, and influence many aspects of AlienVault USM Appliance. Policies use conditions to determine which events are processed by the policy, and consequences to define what will happen when events match the specified conditions.

USM Appliance handles events based primarily on the policies users create to alter its default behavior. By default, events are collected for processing and storage by the USM Appliance Server.

Common Examples of Policies in USM Appliance

There are many ways you can use policies to manage and control event processing within USM Appliance, depending on user, company, and work flow needs. Some practical applications for policies are.

- Send an email notification — You can create a policy to automatically trigger an email to administrators or others whenever a high-risk alarm occurs. For more details, see [Tutorial: Create a Policy to Send Emails Triggered by Events](#).
- Increase the importance of specific events — For a specific IP address or a specific port, you can use policies to generate an alarm whenever events occur that include the IP address of that port, without writing a correlation rule.
- Perform risk assessment and correlation without storing events in the USM Appliance Server — You can avoid storing certain events — such as firewall events you used for correlation on the Server, or instances where the events are no longer needed for correlation — to save space. In some cases, storing them in the USM Appliance Logger long-term for compliance, forensic analysis, or other purposes may work better. For example, see [Tutorial: Create a Policy to Discard Events](#).
- Store events in the USM Appliance Logger without correlating them — In general, you should always allow correlation of events. One exception to this rule might be your security team's use of a honeypot. If you have a honeypot in your network, you do not need USM Appliance to generate alarms for it; you know it will be attacked. Most likely, you would be looking at the logs only as your time permits, because this would be a research project.

- Correlate events and forward them to another USM Appliance Server without storing them — In larger, distributed deployments, you can tier USM Appliance components to improve performance. For example, you can correlate events on a child server and forward them to a higher level USM Appliance Server, or Federation Server, for additional correlation or for storage.
- Reduce false positive alarms — As you collect more events from different external systems, you may run into a scenario that is causing the USM Appliance Server to generate more alarms than you want. You can use policies to filter the events to reduce the number of alarms that are created.

The Policy View

USM Appliance allows you to create and manage policy groups for both external and system events. Policy groups contain sets of certain types of policies grouped together to make them easier to manage. You can access the Policy View page by going to **Configuration > Threat Intelligence > Policy**.

The Policy view has three sections:

- **Default Policy Group** — The Default Policy Group includes no predefined policies. This group is used to hold the policies you create to handle external events. External events are processed by USM Appliance Sensors from systems outside your own network.
- **AV Default Policies** — The AV Default Policies section filters events from the AVAPI user, a service internal to USM Appliance that performs various system tasks. Because these logs only record system processes, their audience consists primarily of AlienVault Technical Support. You can filter such events by highlighting the policy and clicking **Enable**.



Note: In USM Appliance version 5.3.2 and later, the **AVAPI filter** policy is enabled by default.

- **Policies for events generated in the server** — This policy group includes no predefined policies. This group is used to hold the policies you create to handle system events. System events, also called directive events, include any events generated by USM Appliance Server.

The USM Appliance Policy view includes a set of management options that allow you to manage individual policies within any group.

- **New** — Click this button to create a new policy.
- **Modify** — Select an existing policy from the list and click this button to modify that policy.
- **Delete Selected** — Select an existing policy from the list and click this button to delete it.
- **Duplicate Selected** — Select an existing policy from the list and click this button to duplicate it. You can then rename and update the policy as desired and save it.
- **Reload Policies** — Restarts the service used to manage the policies. After you modify or reorder policies for external events, you must reload them. Otherwise, the USM Appliance Server won't recognize the changes.
- **Enable/Disable Policy** — Select a policy from the list and click this button to enable or disable it.

Policy Conditions

Set policy conditions to determine which elements of an incoming event USM Appliance will process. You set these conditions when you create a new policy or modify an existing one. You can set a number of conditions for the default policy group, but events generated in the server only use Event Types.

The screenshot displays the policy configuration interface. At the top, there are fields for 'Policy Rule Name', 'Enable' (Yes/No), and 'Policy Group' (Default policy group). Below this is a table with two main sections: 'CONDITIONS' and 'CONSEQUENCES'.

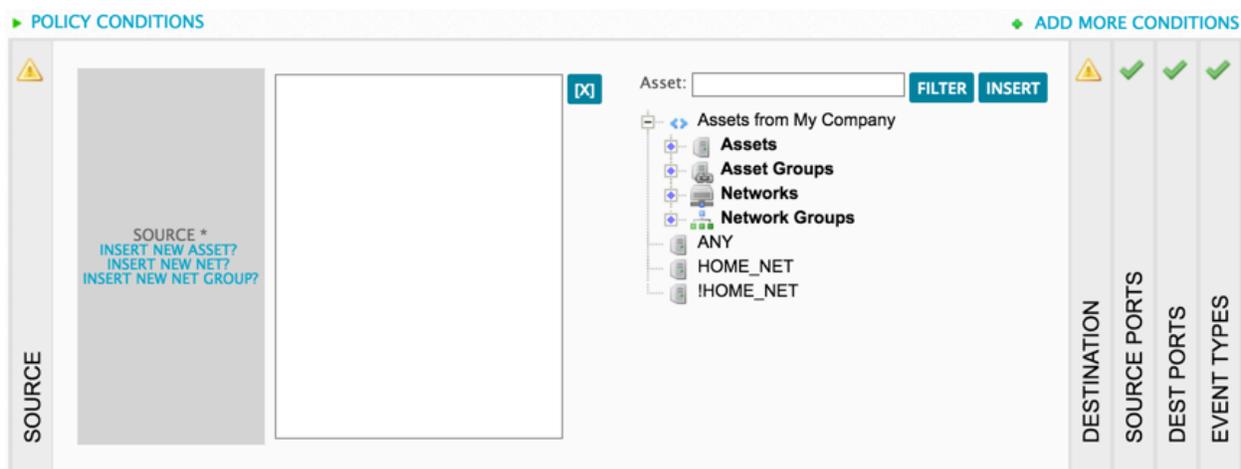
CONDITIONS					CONSEQUENCES			
SOURCE	DEST	SRC PORTS	DEST PORTS	EVENT TYPES	ACTIONS	SIEM	LOGGER	FORWARDING
		ANY	ANY	DS Groups: ANY	No Actions	SIEM (Yes) Set Event Priority: Do not change Risk Assessment: Yes Logical Correlation: Yes Cross-correlation: Yes SQL Storage: Yes	Logger (Yes) Sign: Block	Forward Events (No)

Below the table, there is a 'POLICY CONDITIONS' section with an 'ADD MORE CONDITIONS' button. The 'SOURCE' condition is currently selected, showing a search box with the text 'SOURCE *' and 'INSERT NEW ASSET? INSERT NEW NET? INSERT NEW NET GROUP?'. To the right, there is an 'Asset' search box with 'FILTER' and 'INSERT' buttons, and a tree view of assets including 'Assets from My Company', 'Asset Groups', 'Networks', 'Network Groups', 'ANY', 'HOME_NET', and 'IHOME_NET'. On the far right, there are four vertical tabs: 'DESTINATION', 'SOURCE PORTS', 'DEST PORTS', and 'EVENT TYPES', each with a status indicator (warning or checkmark).

Source and Destination

The Source and Destination allows you to define which Assets, Asset Groups, Networks, or Network Groups will be monitored by the policy. This allows you to tailor policies to focus on events on specific assets or networks. You can add multiple sources or destinations to the condition or if you don't want to limit the number of sources or destinations, you can select **ANY** instead.

In USM Appliance versions 5.4 and later, you can select HOME_NET as a source. HOME_NET, as referred to by its policies usage, is defined by the settings in **Environment > Assets & Groups > Networks**, whereas !HOME_NET are the assets not contained in the HOME_NET group. You can select HOME_NET to include all assets that you are monitoring, or you can use !HOME_NET to exclude all of the assets you are monitoring.



For more detailed instructions, see [Configure Source as a Condition](#) or [Add New Source or Destination](#).

Source Ports and Destination Ports

Source Ports and Destination Ports define the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports that are monitored by the policy. This allows you to monitor packets sent to and from certain port groups in your network.

For more detailed instructions, see [Configure Source or Destination Ports as Conditions](#).

Event Types

Event Types allows you to have granular control on which specific kinds of events the policy will look for. Event types are categorized by two groups:

- DS (Data Source) Groups — Define the data sources for events.
- Taxonomy — Defines the types of events.

The screenshot shows the 'POLICY CONDITIONS' configuration page. At the top right, there is a link to 'ADD MORE CONDITIONS'. Below this, a radio button selection allows choosing between 'DS Groups' (selected) and 'Taxonomy'. Under the 'DS Groups' selection, there is a checked 'ANY *' option. A grid of event type checkboxes is displayed, including: AlienVault NIDS HTTP INSPECT, AlienVault NIDS sigs, AVAPI Event Types, Document files, Executable files, Get IP request, Network anomalies, Sensitive data, and Suspicious DNS, Tor network. A vertical sidebar on the left is labeled 'EVENT TYPES'. A large grey box in the center contains the text: 'DS GROUPS * INSERT NEW DS GROUP? VIEW ALL DS GROUPS'. At the bottom, a note states: '* Directive plugin groups are not allowed in this kind of policy group.'

Event Types — DS Groups

A data source refers to any application or device that generates information which USM Appliance can collect and analyze. USM Appliance organizes data sources for policies affecting events into Data Source Groups. When assembled into a DS group, it makes it easier to incorporate multiple data sources into one policy.

For information about the use of data source plugins in USM Appliance, see "Plugin Data Collection and Normalization" in the Plugin Management section of the *USM Appliance Deployment Guide*.

When you create policies with a data source in mind, you can limit the event types to best suit the policy. If you are creating a policy for a certain plugin, and are only interested in certain events (such as logins, configuration changes, VPN connections, dropped connections), you can select the event types that are most relevant to associate with the plugin. For more detailed instructions, see [Insert a New DS Group Based on Data Sources](#).

Note: Policies belonging to the **Policies for events generated in server** policy group can only include DS Groups comprised of system events.

Event Types — Taxonomy

Taxonomy refers to the classification for security events, using a system based on main categories and subcategories. See [USM Appliance Event Taxonomy](#) for more information.

You can either select general categories, or more specific classifications by relying on the assigned event taxonomies in the database. You can use the **Product Type**, **Category**, and **Subcategory** taxonomy parameters to create a taxonomy condition. Category options change based on which product type is selected. Similarly, the subcategory options change based on which category is selected.

In the example below, only events matching all of the taxonomy parameters would meet the policy condition:

For more detailed instructions, see [Configure Taxonomy as a Condition](#).

Other Conditions

When you click **Add More Conditions** in the bottom-right half of the Policy Conditions page, an additional list of conditions appears.

Sensors

The Sensors policy condition identifies the USM Appliance Sensor that is collecting and normalizing an event. This allows you to specify which sensor or sensors are the source for the events identified for processing by the policy. For example, in distributed deployment, you might want to create a policy for events received from only the sensors that are installed at remote locations.

For more detailed instructions, see [Configure Sensors as a Condition](#).

Reputation

Using Open Threat Exchange **Reputation** data as a policy condition, you can filter events from either the source or destination IP address of an event with more accuracy. To learn more about IP Reputation in USM Appliance, see [OTX IP Reputation Data Correlated with Events](#).

For more detailed instructions, see [Configure Reputation as a Condition](#).

Event Priority

Using **Event Priority** as a policy condition, you can filter events that are from a server according to how reliable the events are. Each event has an assigned priority value. This specifies the importance of the event and defines how urgently the event should be investigated. Priority is a numeric value between 1 and 5, where priority event 1 has no importance, and priority event 5 is of critical importance.

You can use greater than (>), less than (<), or equals to (=) when specifying priority or reliability values for events to set thresholds for the parameter.

Time Range

Time Range sets a period of time in which to match events. When configured, only events that occur during the specified time range are processed by the policy. You can configure the time to a daily, weekly, monthly, or custom time range.

For more detailed instructions, see [Configure Time Range as a Condition](#).

Policy Consequences

You can configure different consequences when creating or modifying a policy. Policy consequences define the ways in which USM Appliance responds to events that trigger the specified policy conditions. You can use consequences to assist you in automatically evaluating elements such as the risk of events, and responding accordingly.



Important: When configuring policy consequences, if you change any of the settings in **SIEM, Logger, or Forwarding**, they will override the default configurations under **Configuration > Deployment > Components > Servers**. The new consequence configuration will apply to all events that match the policy's conditions.

CONSEQUENCES			
ACTIONS ✓	SIEM ✓	LOGGER ✓	FORWARDING ✓
No Actions	SIEM (Yes) Set Event Priority: Do not change Risk Assessment: Yes Logical Correlation: Yes Cross-correlation: Yes SQL Storage: Yes	Logger (Yes) Sign: Block	Forward Events (No)

When setting the consequences policy, keep in mind the following:

- Policies override the default server setting for correlation, event storage, etc. set in servers.
- The Logger option refers to the logger local to this appliance and not to a remote logger (if one was configured).
- If you want to forward events to a remote logger, you must set Forward Events in the forwarding column.

Actions

Actions are performed when the conditions of the designated policy are met. The default is No Actions.

Click the Actions area (green) to display the corresponding section at the bottom of the page. You need to create the actions first before activating them for your policy. See [Create an Action](#) for further information.

SIEM

The SIEM column displays whether or not SIEM processing is active (**Yes**), or inactive (**No**). The default is Yes.

Click the SIEM area (green) to display the corresponding section at the bottom of the page. When SIEM processing is set to Yes, you can also modify the individual options.

► POLICY CONSEQUENCES

ACTIONS SIEM	✓	✓	SIEM	<input checked="" type="radio"/> Yes <input type="radio"/> No
			SET EVENT PRIORITY	Do not change ▾
			RISK ASSESSMENT	<input checked="" type="radio"/> Yes <input type="radio"/> No
			LOGICAL CORRELATION	<input checked="" type="radio"/> Yes <input type="radio"/> No 1)
			CROSS-CORRELATION	<input checked="" type="radio"/> Yes <input type="radio"/> No 1)
			SQL STORAGE	<input type="radio"/> Yes <input checked="" type="radio"/> No 1)
1) Does not apply to targets without associated database. Implicit value is always No for them.				

- **Set Event Priority** — Changes the priority assigned by USM Appliance to events matching the policy conditions, scored from 0-5, with 0 being a non-priority and 5 being the highest importance. The default is Do not change.



Changing the event priority would alter the calculated **Risk**, therefore turning an event into an alarm, or an alarm into an event.

- **Risk Assessment** — Looks at asset value, event priority, and event reliability to evaluate the **Risk** value of the event. The default is Yes.
- **Logical Correlation** — Performs logical correlation as configured in correlation directives. The default is Yes. See also: [Correlation Directives](#).
- **Cross-correlation** — Performs cross-correlation related to events. The default is Yes. See also: [Cross-Correlation](#).
- **SQL Storage** — Stores events in the SIEM database. The default is Yes.

When only **SQL Storage** is set to No, it instructs USM Appliance to perform risk assessment and correlation on the event but do to store it in the SIEM database. The benefit is that you will see an alarm triggered by this event if the calculated risk is above 1, but you will not find this event in the database, saving the storage space.

For more detailed instructions, see [Adjust SIEM Consequences to Process Events](#).

Logger

The Logger consequence determines whether the event will be logged and digitally signed. The default is Yes.

In the policy settings, Logger refers to the local logger, which is included in a USM Appliance All-in-One. When Logger is set to Yes in a policy, USM Appliance will store events locally.

- Line — Digitally signs every log received. This ensures immediate protection from log tampering, but is processing-intensive.
- Block — Digitally signs a block of logs every hour, or whenever the log file is larger than 100 MB. This is the most commonly used signing approach and meets most compliance requirements, but the unsigned block of logs is not secure from being edited until it is signed.

For more detailed instructions, see [Create a Consequence to Log and Sign Events](#).

 **Warning:** When Logger is set to **Yes** in a policy consequence, USM Appliance will send all events that match the policy's conditions to the local logger. This takes precedence over what is configured under **Configuration > Deployment > Components > Servers** (as documented in *Configure the USM Appliance Logger after Deployment*), but only applies to the events that match the policy's conditions.

Forwarding

The Forwarding consequence determines whether to forward events to another USM Appliance Server or Logger. The default is No.

By changing the Forwarding consequence to Yes, you can configure all or a subset of events to be forwarded to an alternate server, such as a federated server.

 **Important:** If you want to forward events to a remote logger, you must set Forward Events in the forwarding column.

For more detailed instructions, see [Create a Consequence to Forward Events](#).

 **Warning:** When Forwarding is set to **No** in a policy consequence, USM Appliance will NOT forward the events that match the policy's conditions. This takes precedence over what is configured under **Configuration > Deployment > Components > Servers** (as documented in *Configure the USM Appliance Logger after Deployment*), but only applies to the events that match the policy's conditions.

Create or Modify a Policy

This section contains subtopics explaining all of the components in how to create an complete a policy:

- [Create an Action](#)
- [Create a New Policy](#)
- [Create Policy Conditions](#)
- [Create Policy Consequences](#)
- [Modify an Existing Policy](#)

Create an Action

You can create actions for USM Appliance to perform on security events. This includes sending an email, executing a script, or opening a ticket. One example of an action could be "When an attack against IP 192.168.1.1 occurs, send an email to an external ticketing system."

To configure an action

1. Go to **Configure > Threat Intelligence > Actions**, select **New**.
2. Type the name of the action in the **Name** field.
3. From the **Context** list, select the context under which the action should occur.
4. In the **Description** field, click on any applicable keywords at the top of the page to automatically add them to the field.

For example, if you wanted to create an action to send an email to an administrator, you could include information from the normalized event in the email message, such as `SRC_IP`, `DST_IP`, `PRIORITY`, and `RISK`.

You can use the following keywords within any field which will be substituted by its matching value upon action execution:

- 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

NAME *	Send_email
CONTEXT *	My Company
DESCRIPTION *	Action to send email
TYPE *	Send an email message
CONDITION	<input checked="" type="radio"/> Any <input type="radio"/> Only if it is an alarm <input type="radio"/> Define logical conditor
FROM: *	alienvault@alienvault.com
TO: *	sec_ops@alienvault.com
SUBJECT: *	USM AlienVault - HIGH priority event
MESSAGE: *	High priority event to an important asset was detected. Date: DATE Source IP address: SRC_IP Destination IP address: DST_IP Event priority: PRIORITY Event risk: RISK

When the action is executed, USM Appliance substitutes the values from the event that triggered the action for the keywords.

Note: You can also use keywords when you want to execute an external program. One example might be an event that invokes a script that sends a shun command to a network firewall to prevent an attacker from making a connection through the firewall at the `DST_IP` address.

5. From the **Type** list, select an action option.

Options include:

- **Send an email message** about an event to a preconfigured email within your organization.

You can also use this option to send notifications by phone messaging services, such as Short Message Service (SMS). However, to do this, you need an external messaging gateway capable of translating email messages to phone messages.

- **Execute an external program** by means of a script.
- **Open a ticket** in USM Appliance's internal ticketing system.

The Actions page expands to include more fields specific to the selection you made.

6. In **Conditions**, indicate under what circumstances the action should occur:

- If you choose **Any** or **Only if it is an alarm**, no new fields display.
- If you choose **Define logical condition**, two new UI fields display:

Python Boolean expression — True or False expressions in Python.

Only on risk increase check box — When checked, this condition must be met for this policy consequence to go into effect.

You can use Boolean comparison operators (==, !=, >, <, >=, <=) and logical operators (AND, OR, NOT) in combination with the provided keywords, such as "Date", "Risk", "Plugin_SID", to define conditions for an action to trigger. For example

The screenshot shows a configuration interface for a condition. At the top, there is a tab labeled 'CONDITION'. Below it, three radio buttons are visible: 'Any', 'Only if it is an alarm', and 'Define logical condition', with the last one selected. A text input field for the 'Python boolean expression' contains the text 'RISK > 3 or PRIORITY == 5'. Below this field, there is a checkbox labeled 'Only on risk increase:' which is currently unchecked. A small note below the input field says '(*) Up to 255 characters'.



Important: When writing an expression, only the following characters are allowed: A-Z, a-z, 0-9, _, ', and ".



Note: Starting from version 5.6, you can also use arithmetic operators, add (+), subtract (-), multiply (*), and divide (/), in an expression.

7. Fill in the fields that appeared after you selected the action type:

To send an email message:

- a. In the **FROM** field, type the email address from which the email message is being sent. This is frequently the USM Appliance administrator.
- b. In the **TO** field, type the email address or addresses to which USM Appliance should send the message.
- c. In the **Subject** field, type a subject for the email. For example, this may reflect the policy's purpose, such as "Escalation of event risk on critical asset."
- d. In the **Message** field, type the content for the email. You can also use the keywords used earlier in the description field.

For a detailed example, see [Tutorial: Create a Policy to Send Emails Triggered by Events](#).

To open a ticket in USM Appliance:

In the **In Charge** field, select either a particular **User** or an **Entity**.

IN CHARGE: * User: OR Entity:

To execute an external program, using a script residing locally:

Type the path to the script in the **Command** field. Once the policy conditions have been met, the program or script will then run.



Important: The best practice is to use non-blocking scripts, as blocking scripts may create response issues or other undesired effects if there is any delay in the script's completion, including the possibility of breaking backup and purging processes.

NAME *	<input type="text" value="Notify Admin of Attack on Critical Servers"/>
CONTEXT *	<input type="text" value="My Company"/>
DESCRIPTION *	<input type="text" value="Shuns an attacker on the firewall."/>
TYPE *	<input type="text" value="Execute an external program"/>
CONDITION	<input type="radio"/> Any <input checked="" type="radio"/> Only if it is an alarm <input type="radio"/> Define logical condition
TO: *	<input type="text"/>
COMMAND: *	<input type="text" value="/usr/admin/python test.py SRC_IP"/>

8. Click **Save**.

Create a New Policy

Policies can be created with actions or without actions in instances where the consequences are SIEM, logger, and forwarding consequences.

To create a new policy

1. Go to **Configuration > Threat Intelligence > Policy**.
2. If you want to create a policy for an external event, click **New** in **Default Policy Group**. If you want to create a policy for a system event, click **New** in **Policies for Events Generated in Server**.
3. Enter a name in the Policy Configuration page.

Policy Rule Name: * ⚠ Enable: * Yes No Policy Group: * Default policy group ⌵

CONDITIONS				
SOURCE ⚠	DEST ⚠	SRC PORTS ✓	DEST PORTS ✓	EVENT TYPES ✓
		ANY	ANY	DS Groups: ANY

4. Configure the conditions that you want the events to match. See [Create Policy Conditions](#) for instructions on each field.
5. Configure what you want to do with the events that have match the conditions. See [Create Policy Consequences](#) for instructions on each field.
6. Click **Update Policy**.
7. Click **Reload Policies**.

🏠 Default policy group: *Default group policy objects*

➕ New
 ✏ Modify
 🗑 Delete selected
 📄 Duplicate selected
🔄 **Reload Policies**
⚙ Enable/Disable policy

Create Policy Conditions

This topic explains how to configure policy conditions for external event policies, using the **Default Policy Group** section on the Threat Intelligence page. The only difference between conditions for directive event policies versus external event policies is that directive event policies have fewer conditions available.

Policy conditions available for both external and directive events

Policy Condition	Used for Directive Events?	Definition
Source		Assets, asset groups, networks, or network groups as the source of an IP address for the event.
Destination		Assets, asset groups, networks, or network groups as the destination of an IP address for the event.
Source Port		TCP/UDP source port of an event.
Destination Port		TCP/UDP destination port of an event.
Event types	✓	Defines events to be processed by this policy. <ul style="list-style-type: none"> Data sources for events are defined by a data source group. Types of events are defined by taxonomy.
Sensors		The USM Appliance Sensor that collected and normalized the event.
Reputation	✓	IP Reputation of the source or destination IP address of an event.
Event priority	✓	Priority and reliability of an event.
Time range	✓	A window of time for event matching.

Create New Policy Conditions

To configure policy conditions for an external event

1. Go to **Configuration > Threat Intelligence > Policy**.
2. In the Default Policy Group section, click **New**.
3. Select one or more conditions that you want to configure for the policy to take effect by doing one of the following:

- On the top half of the policy configuration interface, click on the colored areas under **Source**, **Dest**, **SRC Ports**, **Dest Ports**, or **Event Types** to open the configuration area for each condition.
- On the bottom-half of the policy configuration interface, click one of the vertical labels for **Source**, **Dest**, **SRC Ports**, **Dest Ports**, or **Event Types** to open the configuration area for each condition.

Configure Source as a Condition

To add a source

1. Click on **Assets**, **Asset Groups**, **Networks**, or **Network Groups** and add the desired sources.
2. You can choose **Any** as the source condition if you want the policy to apply to any source. You can also choose **HOME_NET** to include, or **!HOME_NET** to exclude, all assets that you are monitoring.

The selection then appears in the **Source** rectangle under **Policy Conditions**.

Add New Source or Destination

To configure Source or Destination Parameters quickly

1. Click **Insert New Host?**, **Insert New Net?**, or **Insert New Net Group?**



2. Fill in all the configuration information for the new asset.
3. When finished, click **Save**.

Configure Source or Destination Ports as Conditions

To configure one of more source ports as a condition

1. Click the colored **Src Ports** rectangle in the Conditions section of the Policy Configuration page.

Under **Policy Conditions** at the bottom of the page, the Source Ports window appears.

2. Click an asset from the **Ports Groups** tree, or click **Any**.

Your selection appears under Policy Conditions within the **Source Ports** window.

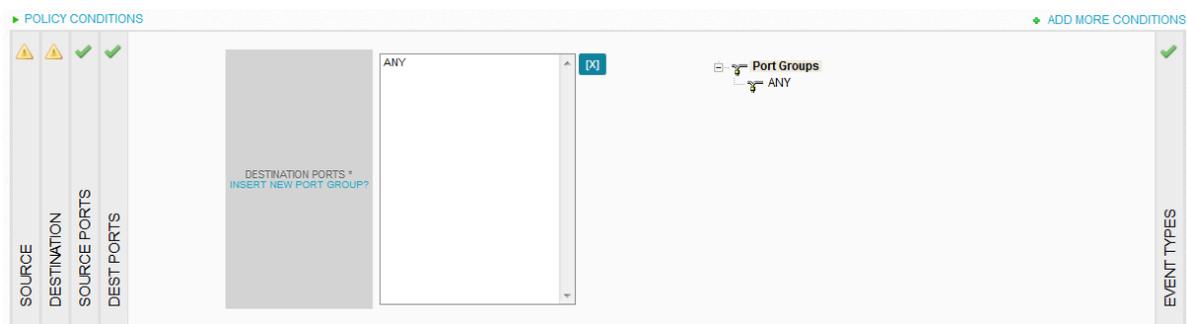
To establish a policy for events destined for certain TCP or UDP ports

1. In the **Conditions** section of the Policy Configuration page, click **Dest Ports**

The **Destination Ports** condition appears under Policy Conditions, at the page bottom.

2. Click a port from the **Port Groups** tree, or click **Any** if you don't need to restrict the event to a specific port.

Your selection appears in the Destination Ports window.



If you do not see the port group listed, click the **Insert New Port Group** link to create one.

Configure an Event Type

This procedure configures a condition for both external and directive event policies.

Event Types define the types of events that will be processed by this policy. In USM Appliance, these consist of data source groups and taxonomy.

You configure an event type by adding either a data source (DS) group or a taxonomy category to it.

Add a DS Group to an Event Type

To add a data source group to an event type

- Select the desired data source groups from the **DS Groups** list by selecting the check box to the left of the group's name. If the box can't be selected, make sure that you deselect **Any**.

Find Out About DS Groups

To find out the available data source groups

1. In the Policy Configuration page, click **Event Types**.
2. Click **View All DS Groups**.

To see more information about a DS Group, click the name of the group to expand it and view a concise description. To edit DS Group information, click the pencil icon at the end of its row.

Insert a New DS Group Based on Data Sources

To insert a new DS group

1. Under Policy Conditions in the DS groups view of Event Types, click **Insert New DS Group**.
2. In the Insert New DS Group dialog box, enter a name for the DS group and select **Add by Data Source**.

3. In the list that displays, click the data sources you want to add to your DS group.

The dialog box now displays the data sources you selected.

4. To include all the event types in the selected data sources (default), click **Update**.
5. Alternatively, if you want to include particular event types, click the pencil icon at the right side of the data source, and complete the following:

- Click the **+** icon to select the event types you want to include.
- You can also use the text box to filter the event types, and then click **Add all**.

Note: A maximum of 150 event types can be selected for each data source in any given DS group. Multiple DS groups can be created for policies requiring more than 150 event types.

INSERT NEW DS GROUP?

Notice:

- Maximum number of Search Results displayed (1000)
- Maximum number of Selected Items (150)

0 Items selected Remove all activity Add all

1 - SAQQARA-CA: Suspicious activity	+
2 - SAQQARA-CA: Suspicious WEB activity	+
9 - SAQQARA-CA: Suspicious SQL activity	+
14 - SAQQARA-CA: Suspicious DNS activity	+
101 - SAQQARA-CA: Suspicious activity ruled out	+
102 - SAQQARA-CA: Suspicious WEB activity ruled out	+
109 - SAQQARA-CA: Suspicious SQL activity ruled out	+
114 - SAQQARA-CA: Suspicious DNS activity ruled out	+
321 - SAQQARA-CA: Periodic RBN activity	+

Empty selection means ANY

SUBMIT SELECTION

Your selections move to the left-hand column of the dialog box.

6. Click **Submit Selection**.
7. Repeat the same steps for the other data sources in the group.
8. Add a description of the new DS Group in the Description field and click **Update**.

The dialog box now shows the entire list of DS groups and reveals details for the DS group you added, consisting of the following:

- Data Source ID
 - Data Source Name
 - Description
 - Event Types
9. (Optional) To add another DS group, click **Add New Group**.
 10. Close the dialog box, which returns you to the Event Types section of the policy. Your newly added DS group appears now as a selection among the DS groups.
 11. Select the new DS group as a condition, along with any others appropriate.

Insert a New DS Group Based on Event Types

To insert a New DS Group Based on Event Type

1. Under Policy Conditions in the DS groups view of Event Types, click **Insert New DS Group**.
2. In the Insert New DS Group dialog box, select **Add by Event Type**.
3. In the **Event Type** field, left-click inside of it to expose the selections.
4. Select the event type and, to see all of the event types of this kind, click **Search**.
5. Select the events for the DS group:
 - To select all events in the list, select **Data Source**.
 - To select particular event types individually, select the check box next to their IDs.
6. Click **Add Selected**.
7. Enter the name for the DS group In the **Please enter a DS Group name** field of the popup of the same name.

The new DS group appears at the bottom of the **Insert New DS Group?** dialog box.

8. To complete this procedure, refer to steps 5 through 8 of [Insert a New DS Group Based on Data Sources](#).

Configure Taxonomy as a Condition

To use taxonomy as a condition

1. In the Conditions section in the top-half of the Policy Configuration page, click **Event Types**.
2. In the Policy Conditions section in the bottom-half of the Policy Configuration page, select **Taxonomy**.
3. Select a product type from the **Product Type** list, or choose **Any**.
4. Select a Category from the **Category** list, or choose **Any**.
5. Select an appropriate **Subcategory**, or choose **Any**.
6. Click **Add New**.

Configure More Conditions

Additional conditions that you can configure for external event policies consist of the following:

- Sensors
- Reputation
- Event Priority
- Time Range



Note: Sensors is the only condition that you cannot use for a policy based on a directive event, since those come through the USM Appliance Server.

To access the additional conditions

- Click **Add More Conditions**.

Configure Sensors as a Condition

To specify a particular USM Appliance Sensor or Any USM Appliance Sensor as a condition for an event

1. At the right-hand top of the Policy Conditions half of the Policy Configuration view, click **Add More Conditions**.
2. Select **Sensors**.
3. Click one of the sensors within the **Sensor list**, or click **Any** to apply the policy to any sensor capturing the event.

Your selection appears within the white **Sensors** field at center.

Configure Reputation as a Condition

By using reputation as a policy condition, you can filter events coming from any of the items in the list with high priority and accuracy.

You can use greater than (**>**) or less than (**<**) when specifying Priority or Reliability values as reputation parameters. For example, if you choose Priority **<** 3 and Reliability **>** 8, USM Appliance adds all the combinations of qualified priority and reliability values as Reputation Conditions.

To add a reputation condition

1. Select the desired **Activity**, **Priority**, **Reliability**, and **Direction** in the Reputation Parameters section.
 - Activity is the type of malicious activity of an IP address that the policy should match.
 - Priority relates to the malicious activity on the part of the IP address. Priority is a number between 1 and 10, where 1 defines a low priority and 10, a high priority.
 - Reliability is a number between 1 and 10, where 1 defines a low reliability (False Positive) and 10, a high reliability (attack in progress), as calculated by OTX IP Reputation.
 - Direction indicates whether or not to match the reputation of the source or destination IP address.
2. Click **Add New**.

Configure Event Priority as a Condition

You can configure Event Priority as a condition for a policy for an external event. However, only AlienVault partners and who have a USM Appliance Federated environment with event forwarding enabled, can use this filter. For details, see the Getting Started Wizard.

To add Event Priority as a condition

1. Click **Event Priority**.
2. Using the guidelines provided in [Policy Conditions](#), set the event priority and reliability as appropriate, using the list boxes.

Configure Time Range as a Condition

You can configure a time range as a condition for a policy for either an external or a directive event.

To add time range as a condition

1. Click **Time Range**.
2. Fill out the frequency, time zone, and start and end dates and times for the events.

The screenshot shows the 'POLICY CONDITIONS' configuration page. A vertical sidebar on the left lists various condition types: SOURCE, DESTINATION, SOURCE PORTS, DEST PORTS, EVENT TYPES, SENSORS, REPUTATION, EVENT PRIORITY, and TIME RANGE. The 'TIME RANGE' option is selected and highlighted. To the right of the sidebar, the 'Timezone' is set to 'US:Eastern'. Below this, there are two main sections: 'BEGIN' and 'END'. The 'BEGIN' section has a frequency dropdown set to 'WEEKLY', a time field set to 7:00, a 'Day of the Week' dropdown set to 'Mon', and a 'Month' dropdown set to 'Jan'. The 'END' section has a time field set to 18:00, a 'Day of the Week' dropdown set to 'Fri', and a 'Month' dropdown set to 'Dec'. There are also radio buttons for 'DAILY', 'MONTHLY', and 'CUSTOM RANGE' options. At the top right, there is a link to 'ADD MORE CONDITIONS'.

Create Policy Consequences

Policy Consequences are the final component to creating a policy, after [Create a New Policy](#) and [Create Policy Conditions](#). Policy Conditions are assigned at the bottom of the Policy's page.

External event consequences can consist of any of the following. You may assign more than one consequence to a policy.

- Actions — [Use an Action as a Consequence to a Policy](#)
- SIEM — [Adjust SIEM Consequences to Process Events](#)
- Logger — [Create a Consequence to Log and Sign Events](#)
- Forwarding — [Create a Consequence to Forward Events](#)

Note: For a directive event, the Logger cannot be configured as a consequence.

Use an Action as a Consequence to a Policy

This task assumes that you or someone else has already created an action that you can reference. For instructions on how to create an action, see [Create an Action](#).

To add an Action to a consequence

1. Go to **Configuration > Threat Intelligence > Policy** and, in the policy you are creating or modifying, click **Actions** under Consequences.
2. Select the action from the **Available Actions**, at right, and add it by clicking the plus (+) sign, or by dragging it to the **Active Actions** section.

ACTIVE ACTIONS		AVAILABLE ACTIONS	
0 items selected	Remove all	Send_Email	Add all <input type="button" value="+"/>

Now the action you selected appears in the **Actions** area of Consequences at the top of the page.

Adjust SIEM Consequences to Process Events

You can choose to make a SIEM consequence for a deeper control over risk assessment, event priority, and correlations. For more details on SIEM as a policy consequence, see [SIEM](#) in Policy Consequences.

To create a SIEM consequence to a policy condition

1. Go to **Configuration > Threat Intelligence > Policy** and, in the policy you are creating or modifying, click **SIEM** under Consequences.

A SIEM window opens under **Policy Consequences** at the bottom of the page.

2. Fill out the form as appropriate.
 - a. **SIEM** — Select **Yes** for SIEM as a consequence.
 - b. **Set Event Priority** — From the **Event Priority** list, select the priority you want USM Appliance to assign to such events. Event priority is from 1 to 5, with 1 being minor and 5 being major, or an attack in progress.

- c. **Risk Assessment** — Indicate whether or not you want USM Appliance to perform risk assessment as a consequence of this policy by selecting **Yes** or **No**.

Risk assessment looks at asset value, event priority, and event reliability. It then assigns a risk based on the value of the asset and type of event.

- d. **Logical Correlation** — Indicate whether or not you want to use logical correlation by selecting **Yes** or **No**.

You use this to create new events from multiple events found by detectors and monitors. These are configured using correlation directives (logical trees combining individual events). Each new event has assigned priority and reliability values define by one directive.

- e. **Cross-Correlation** — Indicate whether or not you want to enable cross-correlation by selecting **Yes** or **No**.

- f. **SQL Storage** — Indicate whether or not you want to enable SQL storage by selecting **Yes** or **No**.

Events detected or generated by USM Appliance are stored in the SQL database by default. Enabling SQL storage means that events matching a policy setting should be stored in the SQL database as well.



Note: It is not required nor desirable for all events to be stored in the database.

Now the SIEM parameters you selected appear in the **SIEM** area of Consequences at the top of the page.



Important: Your changes in the policy will override the default configurations under **Configuration > Deployment > Components > Servers**.

Create a Consequence to Log and Sign Events

By adding a log consequence to your policy, events processed by policies will be sent to the Logger for analysis, compliance, and archiving purposes.

To enable the USM Appliance Logger to log events processed by specific policies

1. Go to **Configuration > Threat Intelligence > Policy** and, in the policy you are creating or modifying, click the colored **Logger** section under Consequences.

A Logger window opens under **Policy Consequences** at the bottom of the page.

2. To enable the Logger to store events caught by your policy (to the local logger), select **Yes**.

Next to **Sign**, you can see that either **Line** or **Block** are selected. (For a detailed explanation of what these do, see [Logger](#) in Policy Consequences.)

Create a Consequence to Forward Events

By enabling the Forwarding consequence, you instruct USM Appliance to forward all or a subset of events, for example, from a remote USM Appliance Server, to a headquarters USM Appliance Server.

To enable event forwarding

1. Go to **Configuration > Threat Intelligence > Policy** and, in the policy you are creating or modifying, click the colored **Forwarding** section under Consequences.

A Forwarding window opens under **Policy Consequences** at the bottom of the page.

2. Select **Yes** to enable forwarding or **No** to disable forwarding.

If you select **Yes**, then select the server you want to forward to.

 **Warning:** Having Logger set to **Yes** and Forwarding set to **No** in a policy consequence will send all events to the local logger. This takes precedence over what is configured under **Configuration > Deployment > Components > Servers** (as documented in [Configure the USM Appliance Logger after Deployment](#)) for all events that fall under the policy's conditions.

Modify an Existing Policy

You can modify any existing policy as needed.

To modify an existing policy

1. From **Configuration > Threat Intelligence > Policy**, click on the policy you want to update.
2. Make any necessary changes in the **Policy Conditions** and **Policy Consequences** sections of the page.

At the top of the page, you can modify the following settings:

- **Policy Rule Name** — This is the name given to the policy.
- **Enable** — Lets you determine if the policy is active or not. After you save the policy modifications, the changes appear in the Policy List view.
- **Policy Group** — Select the policy group with which you want the policy to be associated. To change the default selection, use the list box to select another policy group.

Policy Rule Name: * AVAPI filter ✓ Enable: * Yes No Policy Group: * AV default policies ▾

3. When finished with your modifications, click **Update Policy** to save your changes.
4. Click **Reload Policies**.

Policy Order and Grouping

Policy Order Importance

Policies consist of numbered rules that USM Appliance applies in descending order whenever it processes an event. Similar to the way USM Appliance handles plugin rules, when an event matches a rule, USM Appliance stops looking for other matches, even if they may exist. For this reason, the most specific and restrictive rules should be ordered at the top of the rules list, and generic rules should be ordered at the bottom of the rules list.

In the following example, the second rule is very general, while the third rule is much more specific. This can lead to the third rule not being evaluated. For this reason, you would order the INTERNAL_NMAP rule before the FIREWALL_EVENTS rule.

Default Policy Group: *Default Group Policy objects*

New
 Modify
 Delete selected
 Duplicate selected
 Reload Policies
 Enable/Disable policy

STATUS	ORD [^]	NAME	SOURCE	DESTINATION	SOURCE PORT	DEST PORT
	1	NESSUS_SCANNER	Host-10-128-10-15	ANY	ANY	ANY
	2	FIREWALL_EVENTS	ANY	ANY	ANY	ANY
	3	INTERNAL_NMAP	Host-10-177-16-150	ANY	ANY	ANY

Reorder Existing Policies

This procedure illustrates how to reorder the sequence in which rules are processed.

To re-order existing policies

1. Go to **Configuration > Threat Intelligence > Policy** to view any policies that are configured on your USM Appliance Server.
2. Move the Default Policy Group scroll bar to the right to see additional settings of the configured policies.

When you drag and drop policies a few times to reorder them, you may accidentally end up with duplicated order IDs.

TIME RANGE	TARGETS	SIEM	SET PRIC	RISK A	LOGIC	CROSS	SQL ST	LOGG	SIGN	RESEN
US/Eastern 0h : 0min 23h : 59min	stable	✓	-	✓	✓	✓	✓	✓	Block	⊖
US/Eastern 0h : 0min 23h : 59min	stable	✓	-	✓	✓	✓	✓	✓	Block	⊖

3. To correct this, click **Reorder Policies**.

STATUS	ORD	NAME	SOURCE	DESTINATION	SOURCE
✓	2	Primary Action	HOME_NET	HOME_NET	ANY
✓	3	Secondary Action	ANY	ANY	ANY

Security Events process priority threshold: 0 Reorder Policies

An information popup prompts you to confirm your selection:

Policies are going to be reordered. This action cannot be undone. Are you

sure you want to continue?

4. Click **OK**.
5. Click and drag the policy to move it.

Group Policies to Assign a Correlation Context

Policy groups allow you to group policies for administrative purposes, or to assign policies to a correlation context. Correlation context defines the USM Appliance Sensors and the number of other assets on which to perform correlation.

After initial installation, USM Appliance has one pre-configured policy group, **AV Default Policies**, which filters events from the AlienVault avapi user. However, you will want to create your own policy groups for different situations.

To create your own policy groups

1. Go to **Configuration > Threat Intelligence > Policy**.
2. Click **Edit Policy Groups**.
3. In the **Edit Policy Groups** popup, click **New**.
4. Choose a name for the policy group and assign this policy group either to the entity or context.



Note: You can manage entities and contexts under **Configuration > Administration > Users > Structure**.

Tutorial: Create a Policy to Discard Events

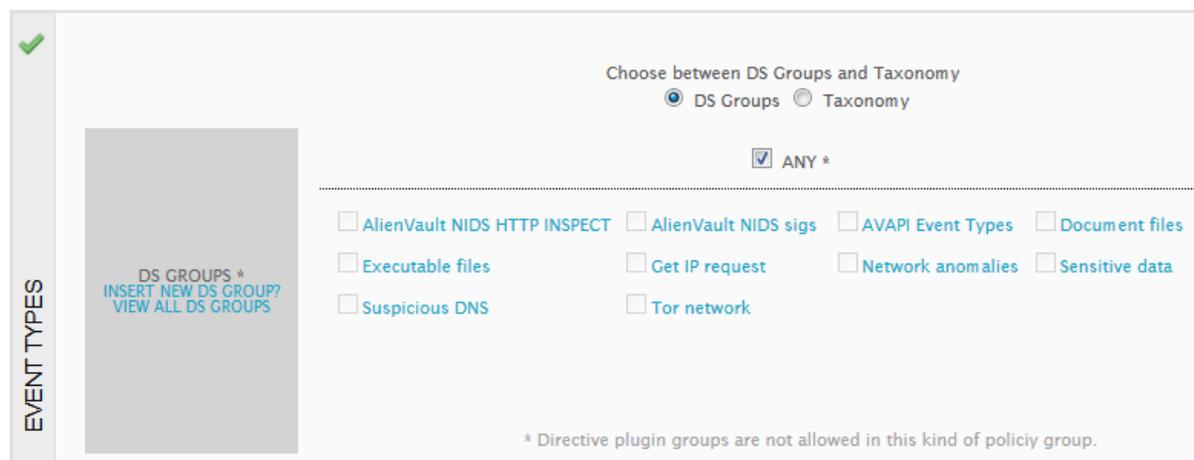
As part of your efforts to reduce the amount of events triggered by non-problematic, non-threat occurrences, you might want to create a policy to make sure that low-priority events don't trigger an alarm. For example, instant messaging programs such as Google Talk and Skype can potentially generate many events based on usage. This has the potential to create a good deal of "noise" in the USM Appliance system. It is generally unnecessary for USM Appliance to process these sorts of events unless a known vulnerability is associated with them.

This process shows you how to discard any events of this type, using Google Talk as an example.

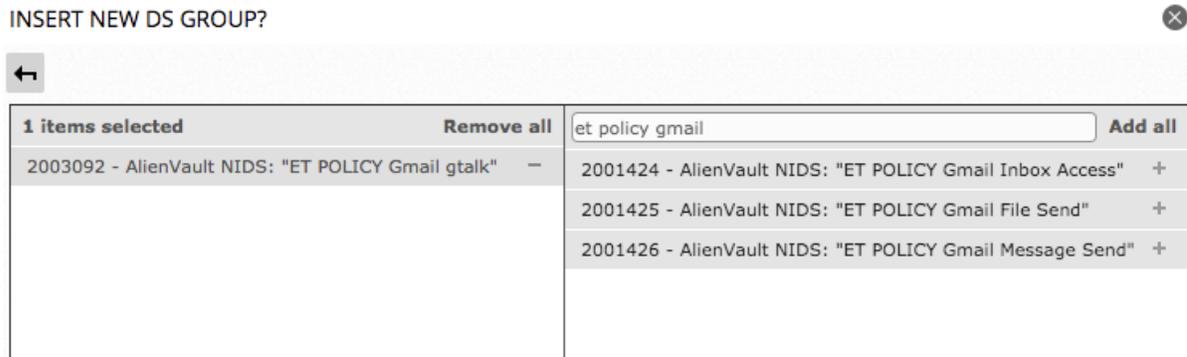
Create a DS Group to Specify Event Types

To filter Google Talk events by using a policy

1. Choose **Configuration > Threat Intelligence > Policy**.
2. On the **Default Policy Group** panel, click **New**.
3. Select the policy conditions: **Source, Destination, Source Ports, and Destination Ports**. Choose **Any** for all these policy conditions.
4. Click **Insert New DS Group?** in the event types tab, to match events related to Google Talk.



5. Write the DS Group Name and add events to the DS group by clicking **Add by Data Source** policy conditions.
6. Select **AlienVault NIDS** data source from the list.
7. Enable editing by clicking the pencil icon (✎)
8. Search for the **ET Policy Gmail GTalk** event and add it by clicking the plus (+) sign.



- Click **Submit Selection** and then **Update** and close the **Insert New DS Group** window.

The new DS group appears in the policy conditions.

- Deselect **Any** and select the newly created DS group.

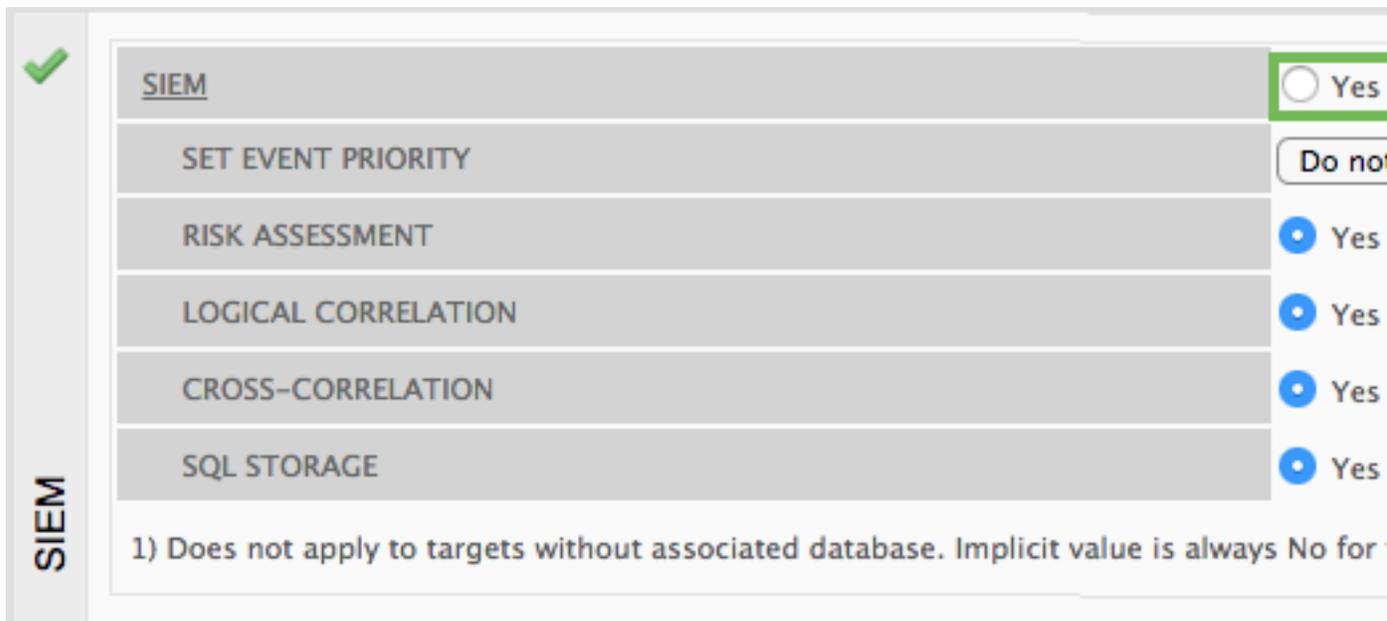
Discard Events

Follow the instructions below to discard Google Talk-related events so that neither risk assessment, logical correlation, cross-correlation, nor SQL storage of events will be performed.

Note: Logging still occurs if the USM Appliance Logger is set to **Yes** in the Policy Consequences section.

To discard Google Talk-related events

1. Open the **SIEM** tab in the policy consequences and select **NO** for SIEM.



2. Enter a name for the policy rule and click **UPDATE POLICY**.
3. Click the **Reload Policies** button on the main policies page to refresh and display the changes.
4. Move the policy to a desired position on the list. See [Policy Order and Grouping](#) for details.

Tutorial: Create a Policy to Send Emails Triggered by Events

For certain important events, you may want a notification to be sent to you or your team to inform them immediately. This process describes how to create the policies that enable these notices.

Create an Action to Send Email

The following procedure shows how to create the action to send an email as a result of your policy. For the emails to be sent successfully, you must also be sure to set up the mail relay server. For further information, see "Connecting Your Corporate Mail Server to USM Appliance" in the Initial Setup section of the *USM Appliance* Deployment Guide.

To create an action to send an email

1. Go to **Configuration > Threat Intelligence**, and click the **ACTIONS** tab.
2. Click **New**.
3. Fill out all of the required fields. In the **TYPE** field, select **Send an email message**.
4. To send the message to multiple recipients, enter their email addresses in the **TO** field, separated with a semi-colon(;).
5. Click **Save** to save your changes when finished.

You can use the following keywords within any field which will be substituted by its matching value upon action execution:

- 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

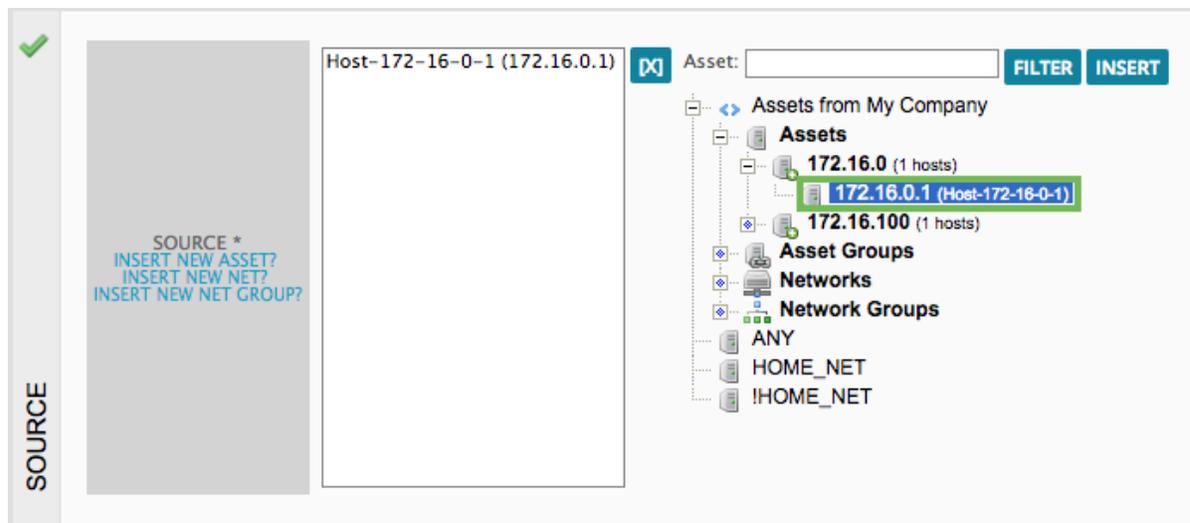
NAME *	Send_email
CONTEXT *	My Company
DESCRIPTION *	Action to send email
TYPE *	Send an email message
CONDITION	<input checked="" type="radio"/> Any <input type="radio"/> Only if it is an alarm <input type="radio"/> Define logical condition
FROM: *	alienvault@alienvault.com
TO: *	sec_ops@alienvault.com
SUBJECT: *	USM AlienVault - HIGH priority event
MESSAGE: *	High priority event to an important asset was detected. Date: DATE Source IP address: SRC_IP Destination IP address: DST_IP Event priority: PRIORITY Event risk: RISK

Create Conditions to Trigger an Email

This procedure configures the conditions for when certain external events target a specific server in your network.

To create policy conditions for external events

1. Go to **Configuration > Threat Intelligence > Policy > Default Policy Group** and select **New**.
2. From the **Policy Conditions** section, choose your source.
3. Select the IP address of the critical server as asset for the destination policy condition. In this example, we are using 172.16.0.1.



4. Click **Add More Conditions**, and select **Reputation** as a policy condition.
5. Change the **Reputation Parameters** values as follows:
 - a. **Activity** — Select Malicious Host.
 - b. **Priority** — Select > 4.
 - c. **Reliability** — Select > 8.
 - d. **Direction** — Select **Destination**, because you want to detect any attacks on the server whose IP address you used as a Destination condition.

6. Click **Add New**.

You can now see both the Destination and Reputation in the upper part of the page.

Assign the Action as a Consequence

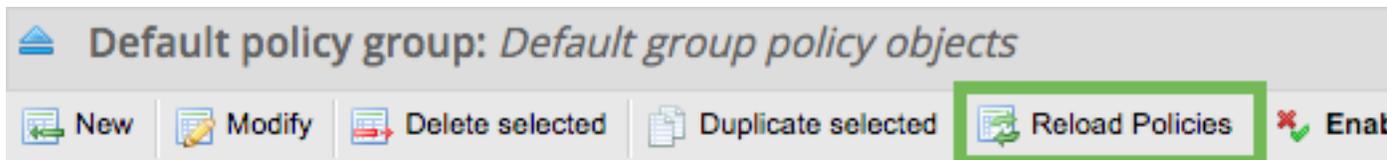
This procedure shows how to link the action to send the email as a consequence.

To create a consequence consisting of an action

1. Go to **Configuration > Threat Intelligence > Policy**.
2. Select the desired policy rule and click the **Modify** button.
3. Scroll down the page and expand the **Policy Consequences** section.
4. In the **Actions** section, select which action you want to assign from the **Available Actions** section on the right.
5. Add it by clicking the plus (+) sign, or by dragging it to the **Active Actions** section.

ACTIONS		INSERT NEW ACTION?
ACTIVE ACTIONS		AVAILABLE ACTIONS
0 items selected	Remove all	Send_Email

- Click the **Update Policy** button to save your changes and exit the policy modify page.
- Click the **Reload Policies** button on the main policies page to refresh and display the changes.



- Move the policy to a desired position on the list. See [Policy Order and Grouping](#) for details.

Tutorial: Create a Policy to Send Emails for Account Lockout Events

You can also use the send an email policy for things such as account lockout events. This is not only helpful for security events, but also for instances such as when you may want to have IT notified of user-related events.

To create a directive for specific user account lockout events

1. Go to **Configuration > Threat Intelligence > Directives > New Directives**
2. In the **New Directive window**, fill out the fields as follows:
 - **Name for the Directive** — User Lockout Notice
 - **Intent** — Environmental Awareness
 - **Strategy** — Bruteforce Authentication
 - **Method** — Attack
 - **Priority** — 3

NAME FOR THE DIRECTIVE

User Lockout Notice

TAXONOMY

Intent: Environmental Awareness

Strategy: Bruteforce Authentication

Method: Attack

PRIORITY

0

1

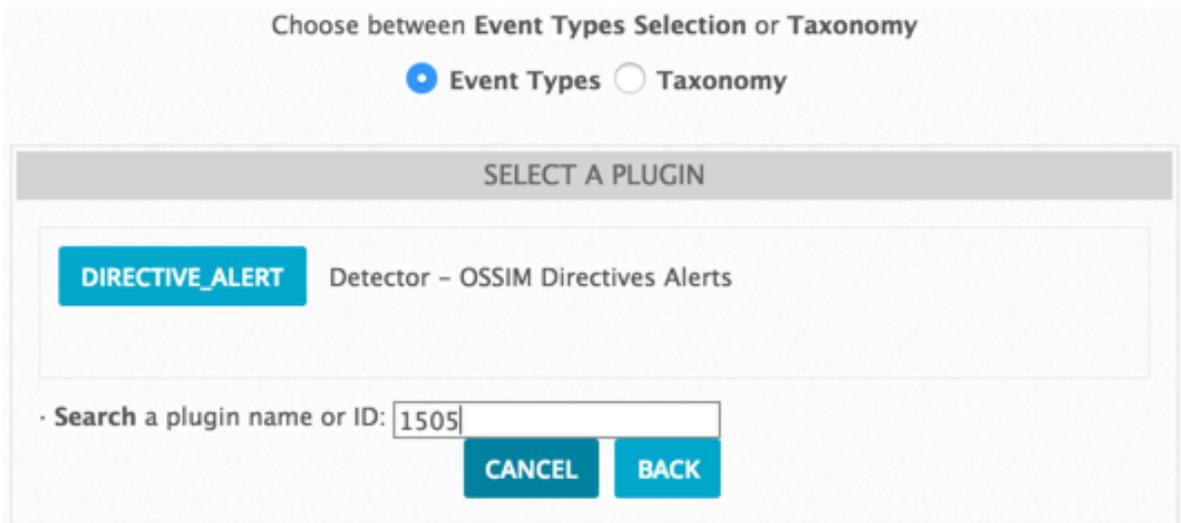
2

3

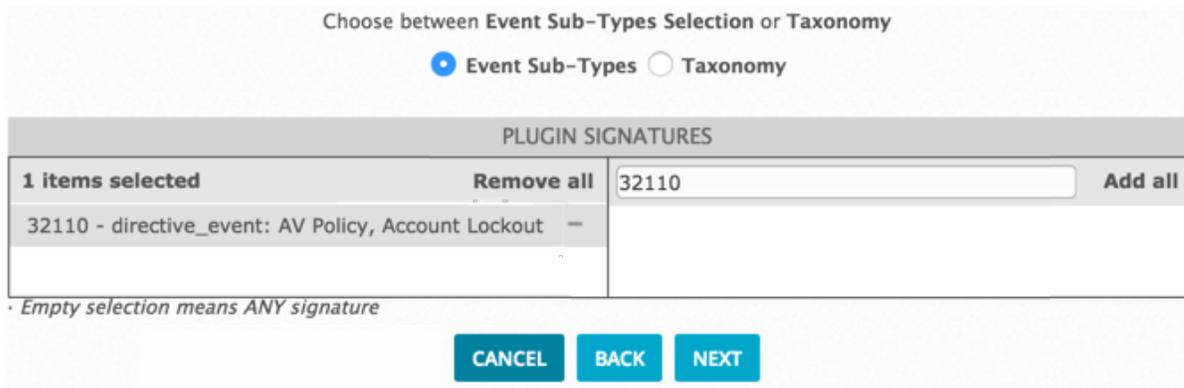
4

5

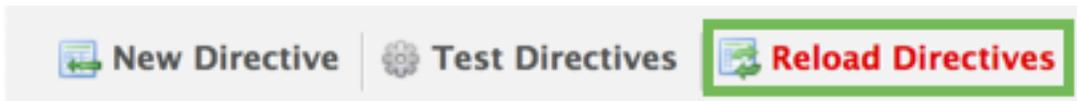
3. Click **Next**
4. Name the rule and click **Next**.
5. Scroll down or use the search at the bottom to find **Directive_Alert** and click on it to select it.



6. In the Event Sub-Types Plugin Signatures window, search for "Lockout" or "32110" to find the **32110 directive event: AV Policy, Account Lockout signature**.
7. Click the plus (+) icon to add it to the left column and click **Next**.



8. In the Network window, either select your desired networks, if any, and click **Next**.
9. Assign a Reliability of 5 and click **Next**.
10. Click **Finish** to save the new directive.
11. Click **Restart Server** on the Directives page to load the newly added directive.



To create the DataSource Group for lockout events

1. Go to **Configuration > Threat Intelligence > Data Source**.
2. Click **Data Source Groups**, and then click **Add New Group**.
3. Give the group a name, such as "Account Lockout Group" and give it a description.
4. Click **Add By Data Source**, search "1505" and click the **1505 directive_alert** data source to add it to the group.
5. Click the pencil icon by the newly added **1505 directive_alert** data source.
6. Search for the recently created lockout directive and click the plus (+) sign to add it to the left column, then click **Submit Selection**.

0 items selected	Remove all	lockout	Add all
		32110 - directive_event: AV Policy, Account Lockout	+
		500001 - Account Lockout	+

Empty selection means ANY

SUBMIT SELECTION

7. Click **Update** to save your changes.

To create the policy

1. Go to **Configuration > Threat Intelligence > Policy**.
2. Scroll down to the **Policies for events generated in server** section and click **New**.
3. Give the new policy a name.
4. Scroll down to **Policy Conditions** and select the account lockout directive you created for the **Event**.
5. Scroll down to **Policy Consequences** and click **Insert New Action**.
6. Fill out the **action name**, **context**, and **description** fields.
7. For **Type**, select **Send an Email Message**.
8. Fill out the **From**, **To**, and **Message** fields.
9. Click **Save**.
10. Click the plus (+) sign on the new action to add it to the policy.

11. Click the **Update Policy** button to save your changes and exit the policy modify page.
12. Click the **Reload Policies** button on the main policies page to refresh and display the changes.
13. Move the policy to a desired position on the list. See [Policy Order and Grouping](#) for details.

Vulnerability Assessment

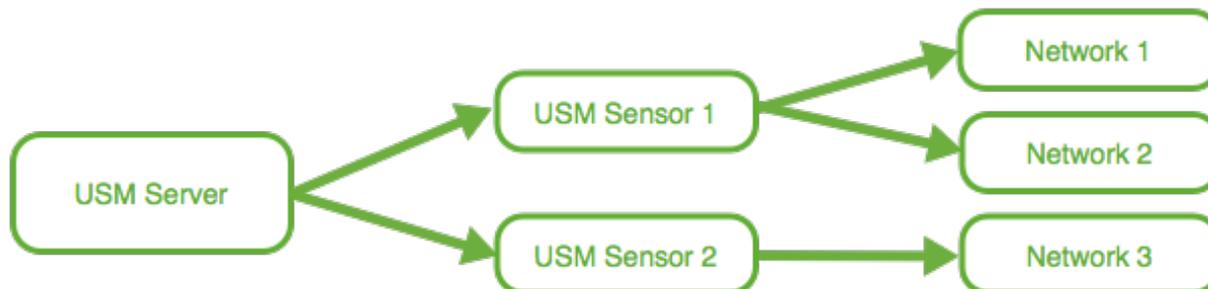
USM Appliance delivers vulnerability assessment as part of a complete package of security monitoring and management capabilities for efficient threat detection. Because to improve security in your network, you first need to know what is vulnerable.

This section covers the following subtopics:

What Is Vulnerability Assessment?	302
Vulnerability Assessment in USM Appliance	302
Vulnerability Risk Factors	302
Vulnerability Scans	303
Viewing the Scan Results	328
Vulnerability Scan Profiles	340

What Is Vulnerability Assessment?

Vulnerability assessment is a functionality used for defining, identifying, classifying and prioritizing the vulnerabilities in your system.



USM Appliance architecture.

The USM Appliance Server controls vulnerability scanning on USM Appliance Sensors. It scans assets in specific networks.

You can select which sensor should scan which network. Alternatively, you can also specify that the first available sensor in your USM Appliance deployment performs the scanning.

Vulnerability Assessment in USM Appliance

The USM Appliance Sensor has a built-in vulnerability scanner that you can use to detect vulnerabilities in critical assets. You then use these discovered vulnerabilities in cross-correlation rules, and when creating compliance and auditing reports.

The USM Appliance Server controls the following scanning functions by the USM Appliance Sensor:

- Running and scheduling vulnerability scans
- Generating and examining reports
- Updating vulnerability signatures

Vulnerability Risk Factors

Discovering a vulnerability by itself is important, but can be of little use without the ability to estimate the associated risk to an asset. For this reason, USM Appliance assigns a risk factor to each vulnerability found in the system, which corresponds with the Common Vulnerability Scoring System (CVSS) v2.0 severity ratings provided by the National Vulnerability Database

(NVD). USM Appliance also compares the detected vulnerability with the Common Vulnerabilities and Exposures (CVE) list and associates it with the CVE ID when a match is found.

Vulnerability Risk Factors and CVSS Scores

Risk Factor	CVSS Scores
High	7.0 – 10.0
Medium	4.0 – 6.9
Low	0.0 – 3.9
Info	0.0 and no CVE associated

You cannot modify the risk factor assigned to each vulnerability. However, you can configure a ticket to be generated when the risk factor reaches a certain value. This value is called Vulnerability Ticket Threshold in USM Appliance. See [Changing the Vulnerability Ticket Threshold](#) for more information.

Vulnerability Scans

In USM Appliance, you can run vulnerability scans from the following pages:

- **Environment > Assets & Groups**, see [Running Vulnerability Scans from Assets](#) for instructions.
- **Environment > Vulnerabilities > Scan Jobs**, see [Creating Vulnerability Scan Jobs](#) for instructions.



Note: Threat intelligence update will not finish if any vulnerability scan job is running, because the update needs to refresh the vulnerability threat database used by the scan.

The **Environment > Vulnerabilities > Scan Jobs** page displays the following sections:

- Running Scans

VULNERABILITIES

OVERVIEW | **SCAN JOBS** | THREAT DATABASE

NEW SCAN JOB | IMPORT NBE FILE | PROFILES | SETTINGS

3 RUNNING SCANS

JOB NAME	OWNER	SCAN TIME	PROGRESS	ACTION
Scan Job 1	admin	RUN >7 mins	<div style="width: 24%;"></div> 24%	
Scan Job 2	admin	RUN >9 mins	<div style="width: 24%;"></div> 24%	
Scan Job 3	admin	RUN >11 mins	<div style="width: 44%;"></div> 44%	Stop current scan job

- Scheduled Jobs

SCHEDULED JOBS

NAME	SCHEDULE TYPE	TIME	NEXT SCAN	STATUS	ACTION
Scheduled scan	Once	23:00:00	2017-11-06 23:00:00	Enabled	Disable scheduled scan job

- All Scans that have completed, including failed scans

ALL SCANS

JOB NAME	LAUNCH TIME	SCAN START TIME	SCAN END TIME	SCAN TIME	NEXT SCAN	REPORTS	ACTIONS
TestDCE2	2021-02-22 10:48:15	2021-02-22 10:50:03	2021-02-22 11:10:59	20 mins	-	(63)	
TestDCE	2021-02-22 10:16:15	2021-02-22 10:18:03	2021-02-22 10:38:55	20 mins	-	(64)	
Test1	2021-02-22 09:43:03	2021-02-22 10:16:02	2021-02-22 10:17:17	1 mins	-	(3)	

The following table displays the fields USM Appliance stores for each scan job.

Scan jobs fields

Field Name	Description
Status	Scan completed or failed.
Job Name	Name given to the scan.
Launch Time	Date and time the scan launched.
Scan Start Time	Date and time the scan started.

Scan jobs fields (Continued)

Field Name	Description
Scan End Time	Date and time the scan ended.
Scan Time	Duration, in minutes, of the completed scan.
Next Scan	Time the next scan is scheduled to start.

The following table displays the post-scan actions USM Appliance may undertake.

Possible post-scan actions

Actions	Meaning
	Displays the results of the report in HTML within the same browser.
	Exports the results of the report in a PDF file. The browser, such as Chrome, may open it in a different tab if it recognizes the file extension.
	Exports the results of the report in an Excel file.
	Exports the results of the scan job in an NBE file.
(n)	Indicates the number of vulnerabilities found on that scan job.
	Changes the owner of the report and makes the scan job visible for a user or entity.
	Re-runs the scan job.
	Deletes the scan job.

Running Vulnerability Scans from Assets

You can run vulnerability scans on individual assets.

The fewer assets to scan, the sooner the scan finishes.



Note: Before scanning a public network space, see "Addendum Notice Regarding Scanning Leased or Public Address Space" under System Overview in the *USM Appliance Deployment Guide*.



Important: Threat intelligence update will not finish if any vulnerability scan is running, because the update needs to refresh the vulnerability threat database used by the scan.

To run a vulnerability scan on selected assets

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset(s) you want to edit. For assistance, see [Selecting Assets in Asset List View](#).
3. Click **Actions**, and then **Run Vulnerability Scan**.

On Vulnerability Scan, the selected assets display at the bottom.

4. Identify the scan job by typing a name in the **Job Name** field.
5. Select a sensor from the **Select Sensor** list.



Important: You can only run up to 5 concurrent scans per USM Appliance Sensor.

6. Select a profile from the **Profile** list or create your own scan profile, see [Vulnerability Scan Profiles](#) for descriptions.
7. In **Schedule Method**, do one of the following:
 - To launch the scan without any delay, keep the default value as "Immediately".
 - To schedule the job to run at a different time, make a selection based on the table below.

USM Appliance vulnerability scan schedules

Schedule Method	Description
Immediately	Launch the scan job without any delay.
Run Once	Run scan once at the specified date and time.
Daily	Run scan every x days at the specified time beginning on the specified day.

USM Appliance vulnerability scan schedules (Continued)

Schedule Method	Description
Day of the Week	Run scan on the specified day and time of the week.
Day of the Month	Run scan on the specified day and time of the month.
Nth week of the month	Run scan on the specified day and time on the Nth week of the month. A week starts on the first day of the month and lasts 7 days.

8. (Optional) Click **Advanced**.

- For authenticated scans, choose **SSH Credential** (UNIX/Linux) or **SMB Credential** (Windows), depending on the operating system of your hosts.



Note: Skip this step for unauthenticated scans. You need to create the credentials first. For assistance, see [Creating Credentials for Vulnerability Scans](#).

- Specify the maximum time (in seconds) that the scan should run.

In USM Appliance version 5.2 and earlier, the default is 28,800 seconds (8 hours).

In USM Appliance version 5.3 and later, the default is 57,600 seconds (16 hours).

- To **send an email notification** after the scan finishes, select **Yes**, and then select **User** or **Entity** as the email recipient.



Important: Be aware of the following when making the selection:

- Admins can view all scans.
- If you are not an admin and you assign the scan to a different user, you can't view this scan yourself.
- If you are an admin and you don't assign the scan to any user or entity, all non-admin users can't view this scan.
- If you are an admin and you assign this scan to a non-admin user, both you and the non-admin user can view this scan, but other non-admin users can't.
- If you assign the scan to an entity, all users who belong to the entity can view the scan.

See [USM Appliance User Accounts](#) for the definition of different user roles.

9. (Optional, available in USM Appliance version 5.3.2 and later) Specify the port numbers you do not want to scan in **Exclude Ports**. Use comma to separate the port numbers but do not use any space between them. For example, "1,33,555,26-30,44".



Note: Using this option slows down the scan because USM Appliance performs additional tasks to exclude the ports you specify.

10. (Optional) To speed up the scanning process, click **Only scan hosts that are alive**.
11. (Optional) If you do not want to pre-scan from a remote sensor, click **Pre-Scan locally**.
12. (Optional) If you do not want to resolve hostnames or FQDN, click **Do not resolve names**.
13. To create the vulnerability scan, click **Save**.

Creating Vulnerability Scan Jobs

By default, USM Appliance runs vulnerability scan jobs without any authentication. They are less thorough and are most appropriate when you want a bird's-eye overview on your assets.



Note: Before scanning a public network space, see "Addendum Notice Regarding Scanning Leased or Public Address Space" under System Overview in the *USM Appliance Deployment Guide*.



Important: Threat intelligence update will not finish if any vulnerability scan is running, because the update needs to refresh the vulnerability threat database used by the scan.

To create a new vulnerability scan job

1. Go to **Environment > Vulnerabilities > Scan Jobs**.
2. Click **New Scan Job**.

VULNERABILITIES

OVERVIEW SCAN JOBS THREAT DATABASE

← CREATE SCAN JOB

Job Name:

Select Sensor:

Profile: [EDIT PROFILES]

Schedule Method:

▶ ADVANCED

Exclude Ports:

Only scan hosts that are alive (greatly speeds up the scanning process)

Pre-Scan locally (do not pre-scan from scanning sensor)

Do not resolve names

Type here to search assets

Assets from My Company

- Assets
- Asset Groups
- Networks
- Network Groups

[X] DELETE ALL

SAVE

3. Identify the scan job by typing a name in the **Job Name** field.
4. Select a sensor from the **Select Sensor** list.

 **Important:** You can only run up to 5 concurrent scans per USM Appliance Sensor.

5. Select a profile from the **Profile** list or create your own scan profile, see [Vulnerability Scan Profiles](#) for descriptions.
6. In **Schedule Method**, do one of the following:
 - To launch the scan without any delay, keep the default value as "Immediately".
 - To schedule the job to run at a different time, make a selection based on the table below.

USM Appliance vulnerability scan schedules

Schedule Method	Description
Immediately	Launch the scan job without any delay.
Run Once	Run scan once at the specified date and time.
Daily	Run scan every x days at the specified time beginning on the specified day.
Day of the Week	Run scan on the specified day and time of the week.
Day of the Month	Run scan on the specified day and time of the month.
Nth week of the month	Run scan on the specified day and time on the Nth week of the month. A week starts on the first day of the month and lasts 7 days.

7. (Optional) Click **Advanced**.

- For authenticated scans, choose **SSH Credential** (UNIX/Linux) or **SMB Credential** (Windows), depending on the operating system of your hosts.



Note: Skip this step for unauthenticated scans. You need to create the credentials first. For assistance, see [Creating Credentials for Vulnerability Scans](#).

- Specify the maximum time (in seconds) that the scan should run.

In USM Appliance version 5.2 and earlier, the default is 28,800 seconds (8 hours).

In USM Appliance version 5.3 and later, the default is 57,600 seconds (16 hours).

- To **send an email notification** after the scan finishes, select **Yes**, and then select **User** or **Entity** as the email recipient.



Important: Be aware of the following when making the selection:

- Admins can view all scans.
- If you are not an admin and you assign the scan to a different user, you can't view this scan yourself.
- If you are an admin and you don't assign the scan to any user or entity, all non-admin users can't view this scan.
- If you are an admin and you assign this scan to a non-admin user, both you and the non-admin user can view this scan, but other non-admin users can't.
- If you assign the scan to an entity, all users who belong to the entity can view the scan.

See [USM Appliance User Accounts](#) for the definition of different user roles.

8. (Optional, available in USM Appliance version 5.3.2 and later) Specify the port numbers you do not want to scan in **Exclude Ports**. Use comma to separate the port numbers but do not use any space between them. For example, "1,33,555,26-30,44".



Note: Using this option slows down the scan because USM Appliance performs additional tasks to exclude the ports you specify.

9. From the asset structure towards the right, select assets, asset groups, or networks to perform the vulnerability scan.



Important: Starting from USM Appliance version 5.3, any scan covering more than 3500 hosts will be split into multiple scan jobs automatically. For example, if you are trying to scan a /16 network that contains 65,536 hosts, it will result in 19 jobs (65,536 / 3500). Each USM Appliance Sensor can run up to 5 jobs simultaneously. You will see 19 reports after the scan has completed.

10. Alternatively, start typing the IP address and USM Appliance fills in the rest as you type. If you want to exclude a specific IP address, prefix your selection with an exclamation mark ("!"), which means do not scan that IP address.

Example:

```
!192.168.2.200
```

11. (Optional) To speed up the scanning process, click **Only scan hosts that are alive**.
12. (Optional) If you do not want to pre-scan from a remote sensor, click **Pre-Scan locally**.
13. (Optional) If you do not want to resolve hostnames or FQDN, click **Do not resolve names**.

- To create the vulnerability scan, click **Save**.

Creating Credentials for Vulnerability Scans

Although optional, we recommend that you use credentials to perform authenticated vulnerability scans. Authenticated scans shouldn't replace network scans, but they use less bandwidth, because they're performed locally, and yield better and more relevant results than unauthenticated scans. They are also more comprehensive and have fewer false positives than unauthenticated scans. For example, authenticated scans check installed software packages, local processes, and services running on the network.

Before running authenticated vulnerability scans in USM Appliance, you need to create some credentials first. For requirements on these credentials, see [System Settings for Authenticated Scans](#). USM Appliance encrypts the credentials using Advanced Encryption Standard (AES) and stores them in the database. The AES algorithm uses Electronic Codebook (ECB) mode and supports a block length of 128 bits.

To create a set of credentials

- Go to **Environment > Vulnerabilities > Overview**, and then click **Settings**.

The screenshot displays two panels from the USM Appliance interface. The left panel, titled 'CREDENTIALS', shows a message 'Credentials not found' and a 'NEW CREDENTIAL' form. The form includes a 'NAME' field, an 'AVAILABLE FOR' section with 'User: nbaena' and 'Entity: - Select one entity -', a 'LOGIN' field, and radio buttons for 'PASSWORD', 'KEY PAIR', and 'PRIVATE KEY'. A 'Choose File' button is next to the 'PRIVATE KEY' option, and a note states '* The Passphrase must be empty'. A 'CREATE CREDENTIAL' button is at the bottom. The right panel, titled 'SETTINGS', shows configuration options: 'Site header logo' (../pixmaps/logo_siempdf.png), 'Portal Branding' (AlienVault), 'Vulnerability Ticket Threshold' (Low), and 'Close Tickets Automatically' (Yes). An 'UPDATE' button is at the bottom.

- In the Name field under New Credential, enter a name for the credential.
- In the Available For section, select one of the following:
 - A single user with permission to use this credential.
 - An entity that allows access by all users who are members of that entity.

4. In the Login field, type the login name for the credential.



Note: To specify a domain, use the syntax "<domain>\<user>", where <domain> is the domain name and <user> is the login name. If you do not specify a domain, USM Appliance uses "WORKGROUP\<user>" because it is the default workgroup name on Windows.

5. Authenticate yourself by selecting one of the following:

- (Default) Type the password for the credential in the Password field.
- Select **Key Pair**, and then click **Choose File** to browse to the location of your private key or key pair file, and then click **Open**.

6. Click **Create Credential**.

A message appears at the top of the page to confirm that you successfully created the new credential.

The new credential appears under Credentials (shown in the following illustration).

SETTINGS

✓
Credential created successfully

CREDENTIALS			
NAME	TYPE	AVAILABLE FOR	ACTION
aa	Password	nbaena	
bb	Password	nbaena	

NEW CREDENTIAL

NAME:

AVAILABLE FOR: User: OR Entity:

LOGIN:

PASSWORD

KEY PAIR

PRIVATE KEY No file chosen

* The Passphrase must be empty

SETTINGS

Site header logo:

Portal Branding:

Vulnerability Ticket Threshold:

Close Tickets Automatically:

To edit an existing credential

1. Click the check mark and pencil icon (🔍✎).
2. In the dialog box that appears, click inside of the empty field below the username or entity (shown).
3. Type or select the appropriate IP address, and then click **Check**.

USM Appliance displays the message:

Checking...

When the authentication process has completed, the Check Credential dialog box displays either "Wrong Credentials" or "Successfully logged in" under Status.

CREDENTIAL CHECK RESULTS		
MESSAGE	SENSOR	STATUS
Checking SSH User/Password	Local	Successfully logged in

To delete a credential

- Click the trash can icon (🗑️).

System Settings for Authenticated Scans

An authenticated scan is a vulnerability testing measure performed from the vantage of a logged-in user. The quality and depth of an authenticated scan depends on the privileges granted to the authenticated user account. The following are the recommended system settings for creating a designated account for authenticated scans.

Asset Scan Credentials and Escalation Options

Operating System	Methods and Credentials	Escalation
Windows	Windows username and password through Server Message Block (SMB)	None
Linux	SSH password or public key authentication	sudo or su
macOS	SSH password or public key authentication	sudo or su

Windows

General System Configurations Overview

Windows Configurations	Settings
General System Configurations	<ul style="list-style-type: none"> Designated domain controller account WMI Service enabled on target Remote Registry enabled on target File and printer sharing must be enabled in the target's network configuration
Group Configurations	<ul style="list-style-type: none"> Designated security group Group scope: Global Scope Group type: Secure Generate registry key
Policy Configurations	<ul style="list-style-type: none"> Designated policy object Policy contains designated domain controller account Designated security group is assigned to policy User rights: Deny local log on, log on through remote desktop services, and write privileges Permissions: Deny permissions for Set Value, Create Subkey, Create Link, Delete, Change Permissions, and Take Ownership

Creating a Windows Admin Account

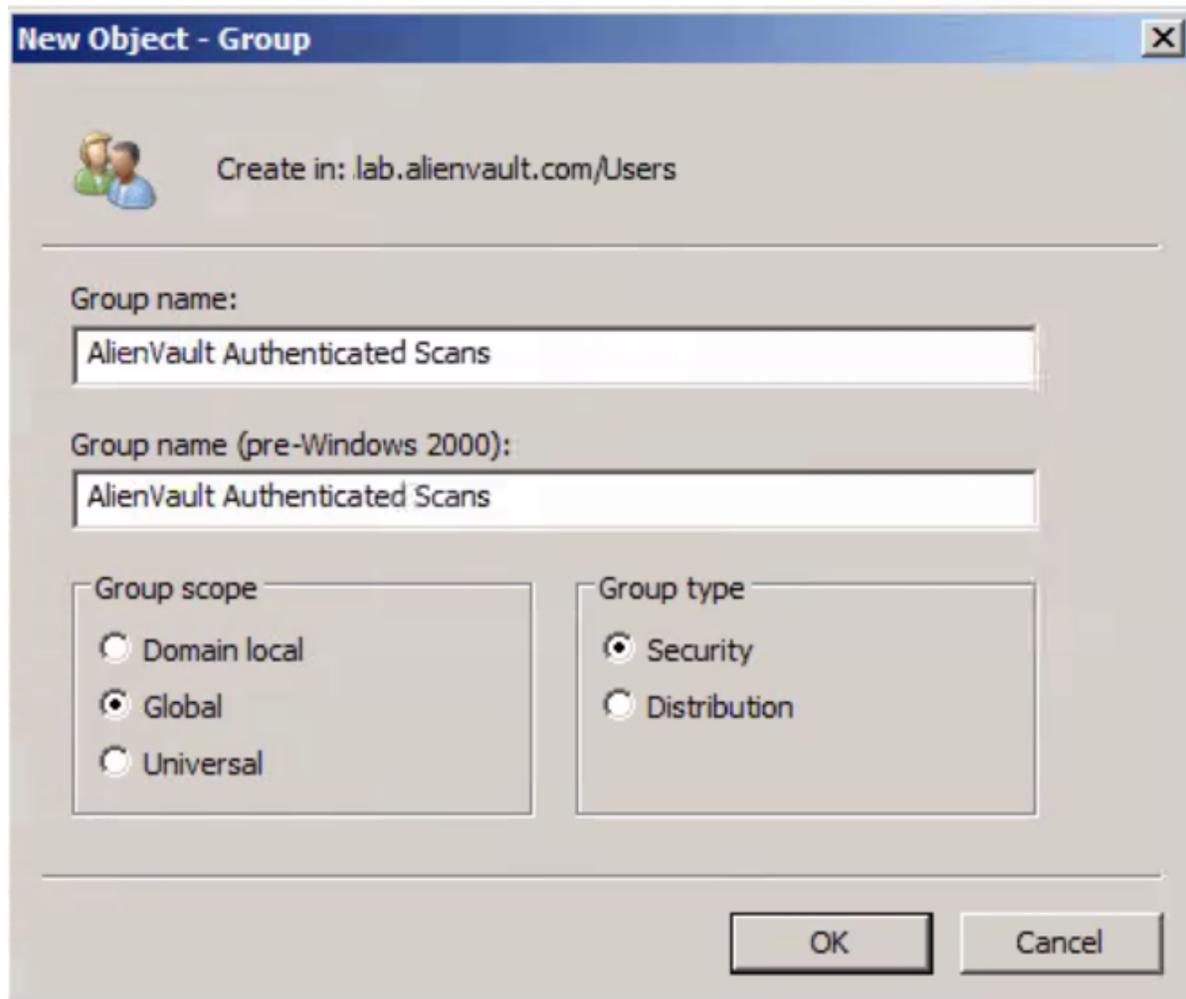
AlienVault recommends that the admin create a designated administrator account solely for the authenticated scans rather than using an established administrator account or a guest account. Create the Windows account using the name **AV Authenticated Account** and a secure password. The account configuration must be set to **Classic: Local Users Authenticate as Themselves**.

For more information about creating credentials for authenticated scans in USM Appliance, see [Creating Credentials for Vulnerability Scans](#).

Creating a Security Group

To create a security group

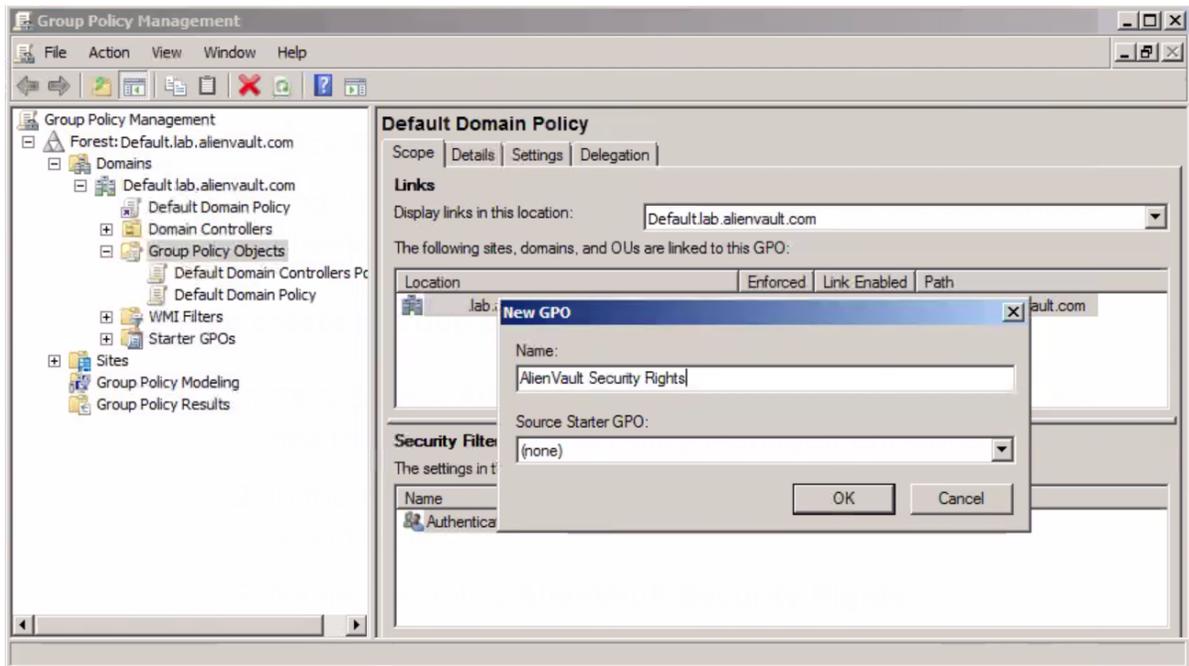
1. Log in to the Active Directory on the Domain Controller.
2. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
3. Click **Select Action > New > Group** to create a new security group.
4. Name the group **AlienVault Authenticated Scan**.
5. For Group Scope select **Global**.
6. For Group Type select **Security**.
7. Click **OK** to add the group.



8. Add the account that you will be using for the authenticated scans to the **AlienVault Authenticated Scan** group.

To create a group policy

1. Click **Start > All Programs > Accessories > Run**, and then type `gpmmc.msc` in the text box to open the Group Policy Management window.
2. In the Group Policy Management window, right-click **Group Policy Objects**, and then select **New**.
3. Name the policy **AlienVault Security Rights**, and then click **OK**.



4. In the Group Policy Management Editor, click the **AlienVault Security Rights** policy to open the policy in the right pane.
5. Click on the **Scope** tab, and then in the Security Filtering section, click **Add** to insert the group.
6. In the Enter the Object Name to Select field, add the **AlienVault Authenticated Scan** group to the policy, and then click **OK**.

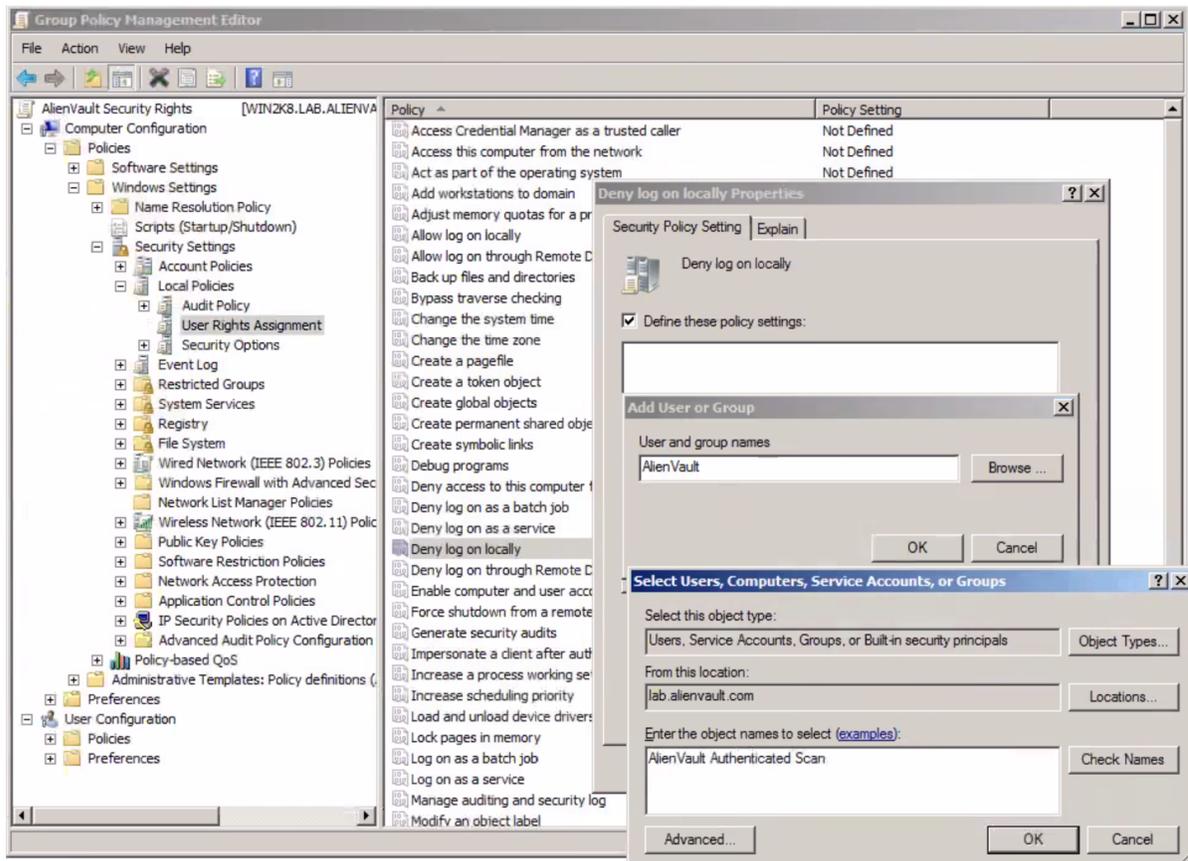
Configuring Policies

The following configurations are optional steps you can take in the Group Policy Management Editor to remove unnecessary user rights. These steps are not required for running the authenticated scans, but they do provide extra measures of internal security.

To deny local logins

1. Right-click on the **AlienVault Security Rights** policy, and then select **Edit**.
2. In User Rights Assignment, double-click **Deny Log on Locally**.
3. Click **Add User or Group**.

4. Click **Browse**, enter **AlienVault Authenticated Scan**, and then click **Check Names**.
5. Click **OK**.

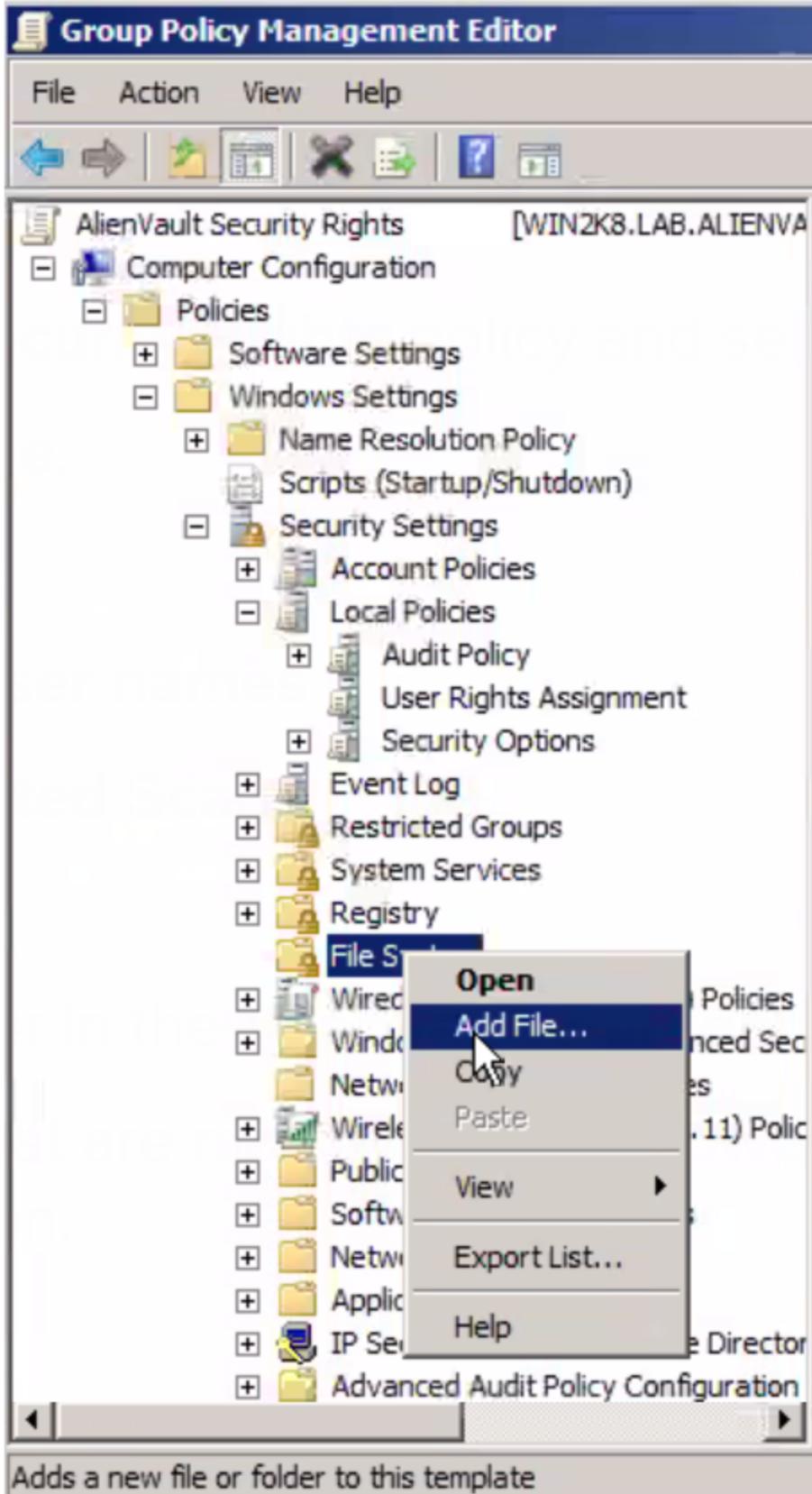


To deny Remote Desktop Services log

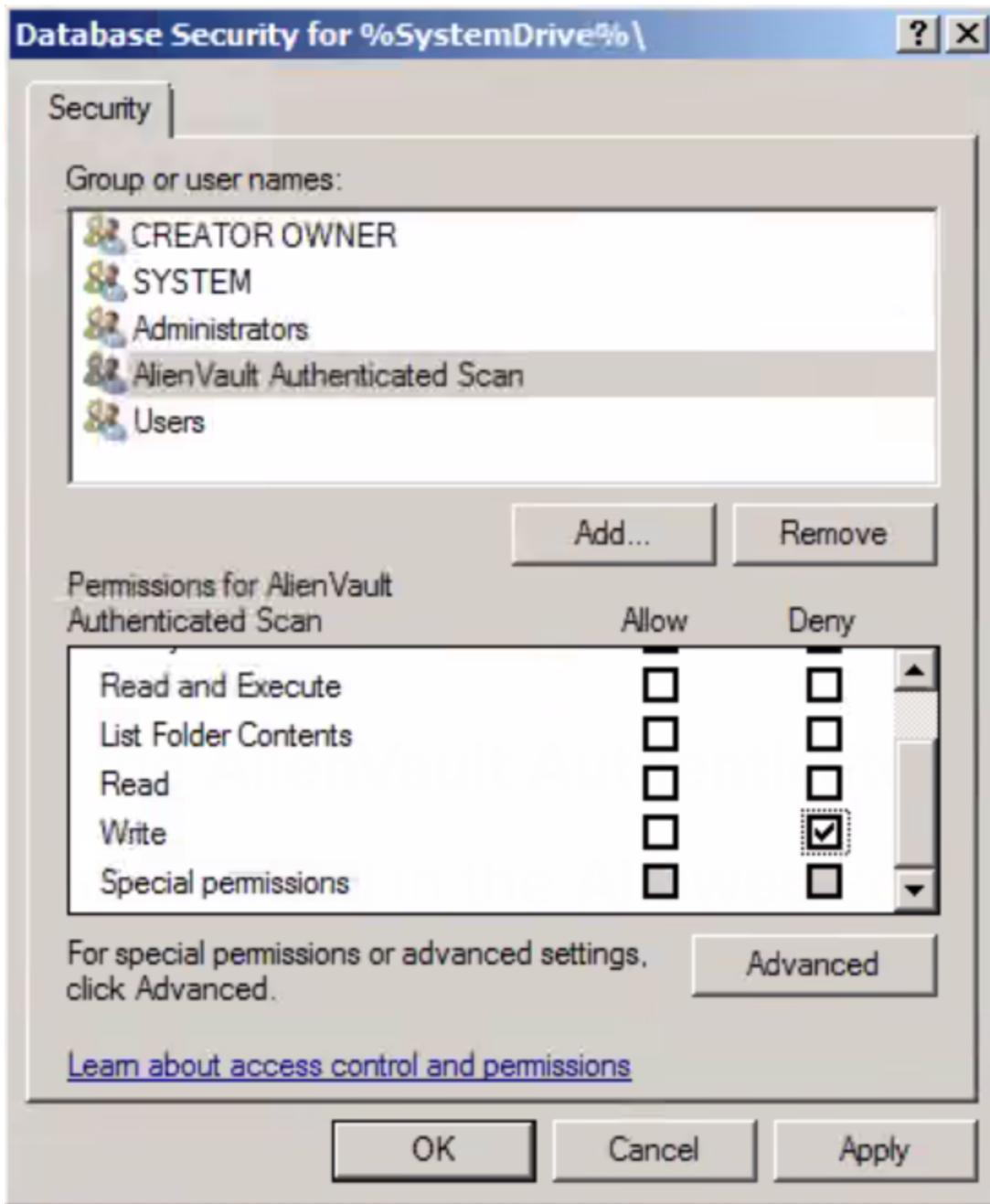
1. Right-click the **AlienVault Security Rights** policy, and then select **Edit**.
2. In User Rights Assignment, double-click **Deny Log Through Remote Desktop Services**.
3. Select **Define These Policy Settings**.
4. Click **Add User or Group**.
5. Click **Browse**, enter **AlienVault Authenticated Scan**, and then click **Check Names**.
6. Click **OK**.

To configure permissions

1. Right-click **File Systems**, and then select **Add File**.



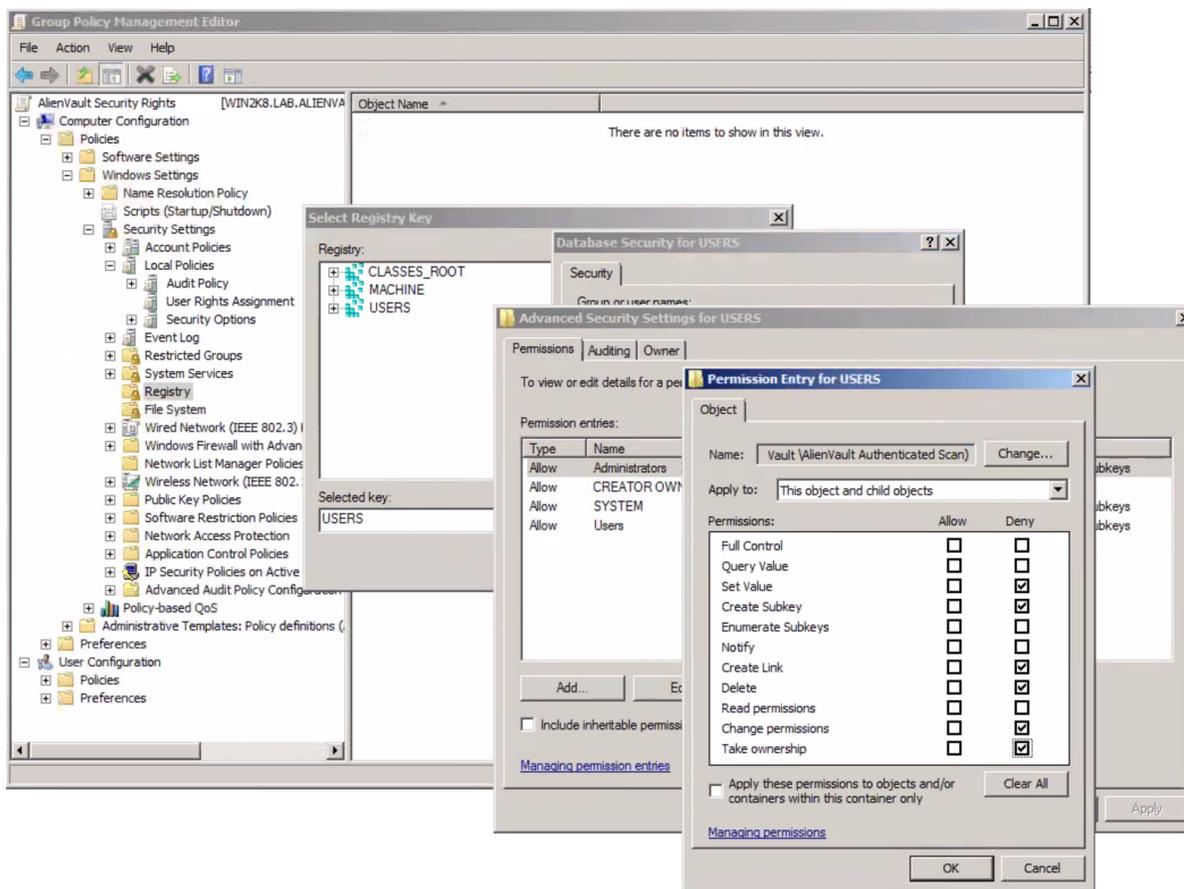
2. Enter %SystemDrive%.
3. Under Group or User Names, click **Add**.
4. Enter **AlienVault Authenticated Scan**.
5. Click **OK**.
6. In the AlienVault Authenticated Scan group, select the authenticated user.
7. Deselect any permissions that are marked in the **Allowed** column, and then select **Deny** for the Write permission.
8. Click **OK**.



9. In the Object window, select **Configure This File or Folder Then** and **Propagate Inheritable Permissions to All Subfolders and Files**, and then click **OK**.

To configure registries

1. Click **Registry**, and then select **Add Key**.
2. Select **Users**, and then click **OK**.
3. Click **Advanced**, and then click **Add**.
4. Enter the **AlienVault Authenticated Scan** group, and then click **OK**.
5. In the Permissions Entry Objects window's **Apply To** field, select **This Object and Child Objects**.
6. In the Permissions section below, select **Deny** for **Set Value, Create Subkey, Create Link, Delete, Change Permissions, and Take Ownership**. No checkboxes should be set to **Allow**.
7. Click **OK** and confirm the changes.



8. Select **Configure This Key Then** and **Propagate Inheritable Permissions to All Subkeys** radio buttons, and then click **OK**.
9. Repeat these steps for the **Machine** and **Classes Root Registries** as well.

Linux

To perform authenticated scans on USM Appliance from a Linux system, the user must have root privileges. The Linux login is performed through SSH, while USM Appliance performs the authentication either with a password or an SSH key stored in USM Appliance. The Linux account used for authenticated scans must be able to perform `uname` commands and read and execute Debian (.deb and .dpkg) or Red Hat (.rpm) files. Public Key Authentication must not be prohibited by the SSH daemon with the line `PubkeyAuthentication no`.

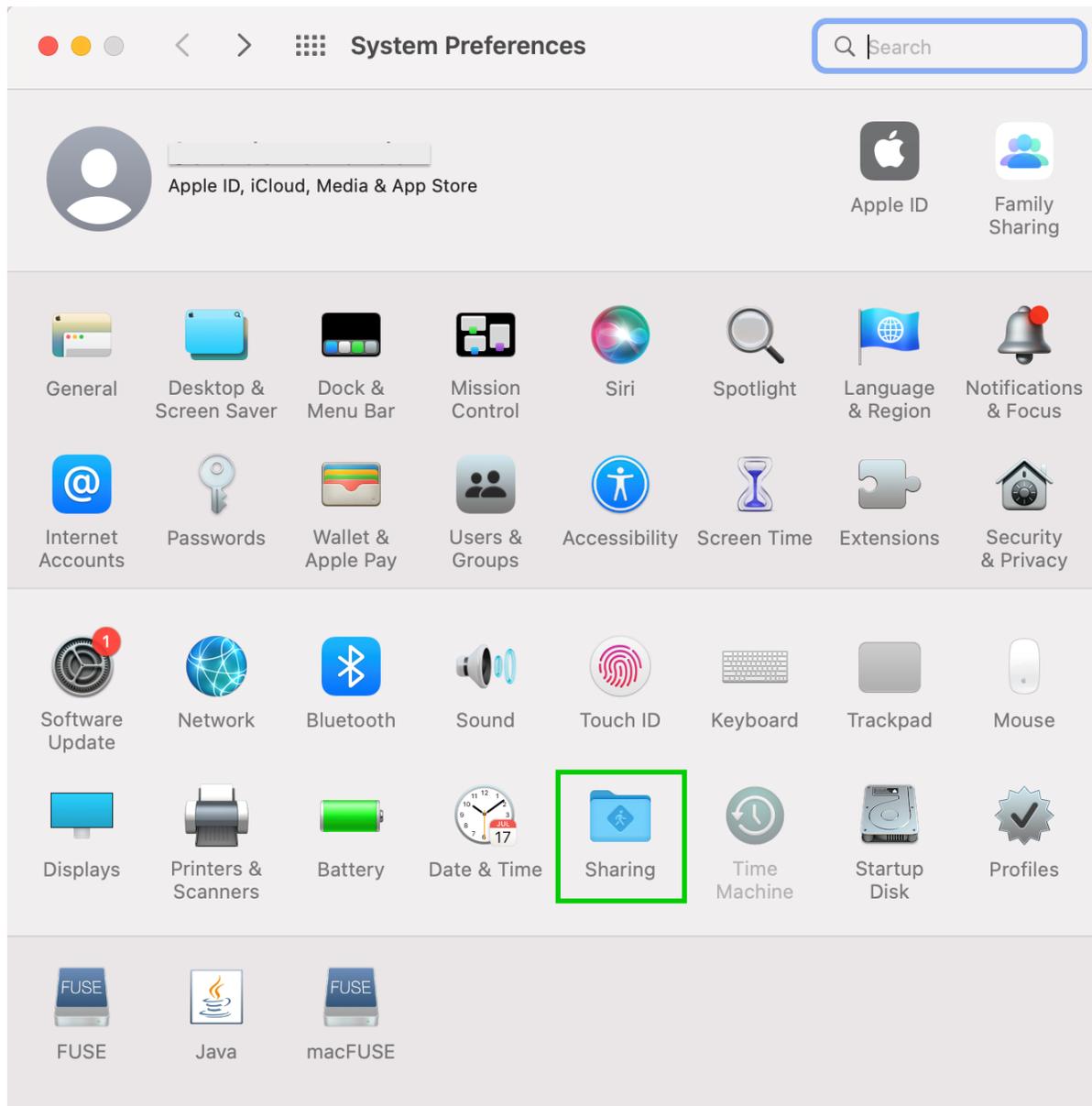
For more information about creating credentials for authenticated scans in USM Appliance, see [Creating Credentials for Vulnerability Scans](#).

macOS

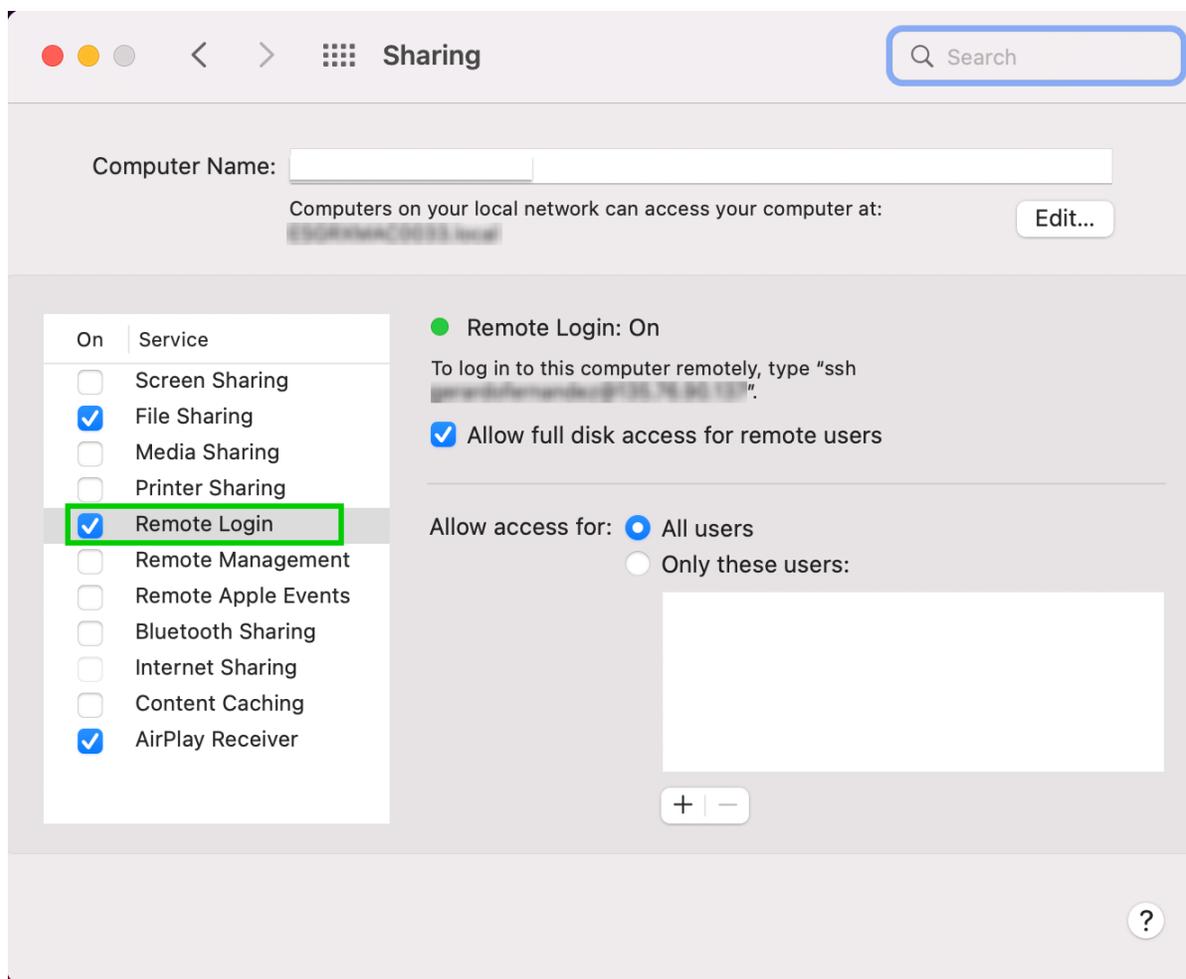
To perform authenticated scans on USM Appliance from a macOS, the user must have root privileges.

To enable SSH access on macOS

1. Open **System Preferences**, and then select **Sharing**.



2. Select **Remote Login**.



For more information about creating credentials for authenticated scans in USM Appliance, see [Creating Credentials for Vulnerability Scans](#).

Viewing the Scan Results

This section covers the following subtopics:

- [Vulnerabilities Views](#)
- [Viewing the Scan Results in HTML](#)
- [Viewing the Scan Results in PDF](#)
- [Viewing the Scan Results in Excel](#)
- [Importing Scan Results](#)
- [Comparing the Results from Two Scans](#)

Vulnerabilities Views

This overview examines the vulnerability statistics across all scans.

You can also display the results, called scan reports, as HTML or export them as a PDF or Excel file. To see the summary of vulnerabilities, go to **Environment > Vulnerabilities > Overview**.

VULNERABILITIES ?

OVERVIEW **SCAN JOBS** THREAT DATABASE

PROFILES **SETTINGS**

BY SEVERITY **BY SERVICES - TOP 10**

■ High [8]
■ Medium [1]
■ Low [81]

TOP 10 HOSTS **TOP 10 NETWORKS**

bat50 [84]

Host-172-16-0-1 [6]

▼ CURRENT VULNERABILITIES

ASSET VULNERABILITY DETAILS

NEW SCAN JOB Service Free text Host/Net **FIND**

HOST - IP	DATE/TIME	PROFILE	CRIT	HIGH	MED	LOW	INFO	
All	-	-	0	8	1	81	0	VIEW PDF EXCEL
stable (172.16.100.1)	2015-08-05 03:42:12	Default	0	4	0	38	0	VIEW PDF EXCEL DELETE
bat50 (172.16.100.1)	2015-08-05 03:40:35	Default	0	4	0	38	0	VIEW PDF EXCEL DELETE
Host-172-16-0-1 (172.16.0.1)	2015-08-04 07:09:54	Default	0	0	1	5	0	VIEW PDF EXCEL DELETE

▼ REPORT HISTORY

SCAN REPORTS DETAILS

Date/Time Job Name Host/Net **FIND**

DATE/TIME	JOB NAME	TARGETS	PROFILE	CRIT	HIGH	MED	LOW	INFO	
2015-08-05 03:42:12	dd	stable	Default	0	4	0	38	0	VIEW PDF EXCEL DELETE PRINT SHARE
2015-08-05 03:40:35	cc	bat50	Default	0	4	0	38	0	VIEW PDF EXCEL DELETE PRINT SHARE
2015-08-04 07:32:50	bb	stable	Default	0	4	0	38	0	VIEW PDF EXCEL DELETE PRINT SHARE
2015-08-04 07:09:54	aa	Host-172-16-0-1	Default	0	0	1	5	0	VIEW PDF EXCEL DELETE PRINT SHARE

Vulnerabilities Assessment Overview sections

Section Name	Description
By Severity	<p>A pie chart that displays:</p> <ul style="list-style-type: none"> • All current vulnerabilities by severity, in percentages. • Number of vulnerabilities found (shown in square brackets).
By Services-Top 10	<p>A pie chart that displays vulnerabilities from the top 10 services.</p> <p>Click within the chart to filter the vulnerabilities related to a service. And then click Overview to refresh the view of all services.</p>
Top 10 Hosts	<p>A horizontal bar graph displays the top 10 hosts with the most vulnerabilities.</p> <p>Click a host to filter the vulnerabilities related to that host. And then click Overview to refresh the view of all hosts.</p>
Top 10 Networks	<p>A horizontal bar graph displays the top 10 networks with the most vulnerabilities.</p> <p>Click a network to filter the vulnerabilities related to that network. And then click Overview to refresh the view of all networks.</p>
Current Vulnerabilities	<p>Summarizes the vulnerabilities found in the scan jobs.</p> <p>The first line refers to all scans.</p> <p>The next lines refer to every host.</p> <p>Vulnerabilities are classified by importance (Critical, High, Medium, Low and Info).</p> <p>For related information, see Changing the Vulnerability Ticket Threshold.</p>
Report History	<p>Displays the results from every scan. (See Viewing the Scan Results.)</p> <p>Classifies vulnerabilities by importance (Critical, High, Medium, Low and Info).</p> <p>For related information, see Changing the Vulnerability Ticket Threshold.</p>

The Vulnerabilities Assessment Overview page includes the buttons, shown in the following table.

Vulnerabilities Assessment Overview page button meanings

Button Name	Definition
Profiles	Opens the Vulnerability Scan Profiles page. (See Vulnerability Scan Profiles for details.)
Settings	Opens the Vulnerability Scan Settings page. (See Creating Credentials for Vulnerability Scans for details.)
New Scan Job	Creates a scan job. (See Creating Vulnerability Scan Jobs for details.)

You can also see the summary of vulnerabilities by going to **Dashboards > Overview > Vulnerabilities**.

Current Vulnerabilities — Asset Vulnerability Details

The **Asset Vulnerability Details** section summarizes all current vulnerabilities found in the scan jobs by the number of vulnerabilities, in descending order. The first line refers to all scans and the following lines refers to the scans done on every host.

▼ CURRENT VULNERABILITIES

ASSET VULNERABILITY DETAILS

[NEW SCAN JOB](#) Service Free text Host/Net [FIND](#)

HOST - IP	DATE/TIME	PROFILE	CRIT	HIGH	MED	LOW	INFO	
All	-	-	0	8	1	81	0	  
stable (172.16.100.1)	2015-08-05 03:42:12	Default	0	4	0	38	0	  
bat50 (172.16.100.1)	2015-08-05 03:40:35	Default	0	4	0	38	0	  
Host-172-16-0-1 (172.16.0.1)	2015-08-04 07:09:54	Default	0	0	1	5	0	  

Fields and descriptions for Asset Vulnerability Details

Field	Description
Host-IP	Shows the hostname and IP of the host. The first line 'All' summarizes all hosts.
Date/Time	Shows the exact date and time that the scan occurred.
Owner	Indicates the user who created the scan.
Profile	Indicates the chosen profile to run the scan.

Fields and descriptions for Asset Vulnerability Details (Continued)

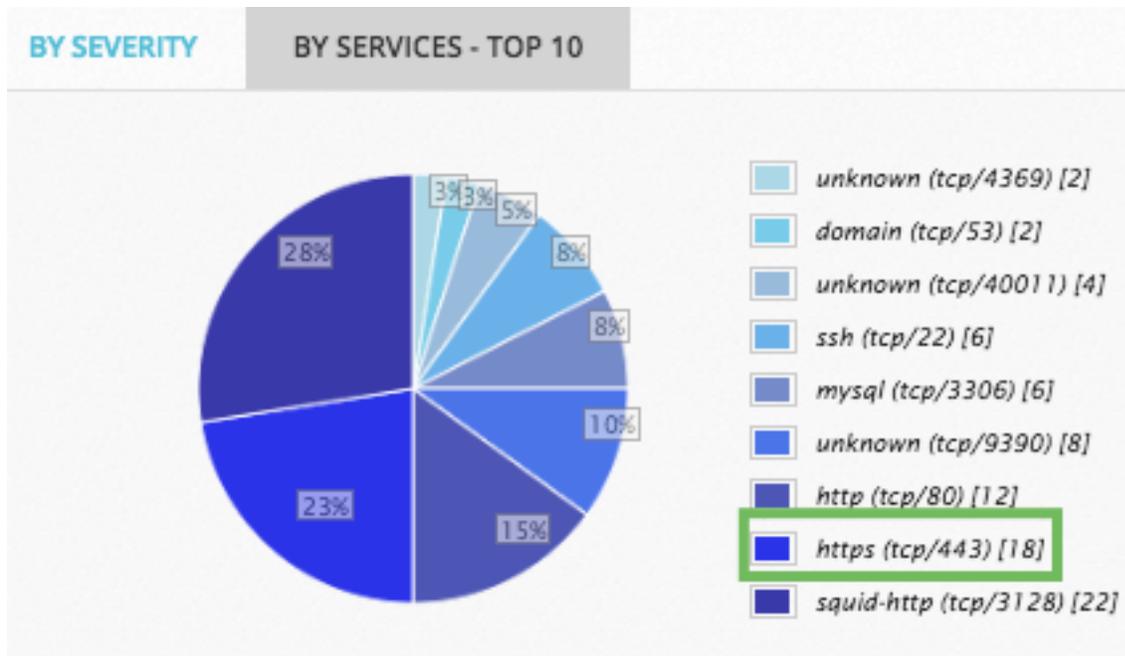
Field	Description
	Displays the number of Critical vulnerabilities found in the latest scan.
	Displays the number of High vulnerabilities found in the latest scan.
	Displays the number of Medium vulnerabilities found in the latest scan.
	Displays the number of Low vulnerabilities found in the latest scan.
	Displays the number of Info vulnerabilities found in the latest scan.
	Results of the scan job in HTML within the same browser.
	Exports the results of the scan job to a PDF file. The browser, such as Chrome, may open it in a different tab if it recognizes the file extension.
	Exports the results of the scan job to an Excel file.
	Deletes the report.

For details about the threshold of vulnerabilities, see [Changing the Vulnerability Ticket Threshold](#).

To filter the data

- In the empty box above the table, enter an IP address of a host/network (default), the name a service, or a free text. Use the following definitions to help you select which one to use:
 - Host/Net:** Searches the IP address of a single host or a range of IP addresses in a sub-net (for example, `10.80.50.73`, `10.80.50.1/24`).
 - Service:** Searches the security service identified in the vulnerability (for example, `ssh`, `http`, or `https`, as seen in the By Services -Top 10 pie chart).
 - Free text:** Searches the details of a vulnerability using free text.
- Select the corresponding radio button.
- Click **Find**.

Another way to filter the data is by using the pie chart above the **Current Vulnerabilities**. In the following example, we can see that the `https` service has 18 vulnerabilities (between the square brackets):



To see which hosts have such vulnerabilities

1. Click the text that reads **https**.

The page refreshes with the text *https* populated in the search box and the option **Service** selected.

Only the host(s) with the https vulnerabilities display.

VULNERABILITIES

OVERVIEW SCAN JOBS THREAT DATABASE

THREATS FILTER

DATE RANGE KEYWORDS CVE ID RISK FACTOR

SEARCH

THREAT FAMILY	INFO-7	LOW-6	MEDIUM-3	HIGH-2	SERIOUS-1	TOTAL
AIX Local Security Checks	0	0	1	0	0	1
Brute force attacks	0	4	1	6	0	11
Buffer overflow	0	0	12	158	350	520
CentOS Local Security Checks	0	12	275	1,254	838	2,379
CISCO	0	0	7	24	7	38
Compliance	0	6	0	0	0	6
Credentials	0	5	0	0	0	5

2. To check vulnerabilities in details, you can look at the HTML report or export a PDF or Excel file.

Viewing the Scan Results in HTML

To view the results of the scan report in HTML within the same browser

1. Go to **Environment > Vulnerabilities > Overview**.
2. Click **Report History** if that section has not been expanded.

REPORT HISTORY

SCAN REPORTS DETAILS Critical

Date/Time Job Name Host/Net FIND

DATE/TIME	JOB NAME	TARGETS	PROFILE	CRIT	HIGH	MED	LOW	INFO	
2015-08-05 03:42:12	dd	stable	Default	0	4	0	38	0	     
2015-08-05 03:40:35	cc	bat50	Default	0	4	0	38	0	     
2015-08-04 07:32:50	bb	stable	Default	0	4	0	38	0	     
2015-08-04 07:09:54	aa	Host-172.16-0-1	Default	0	0	1	5	0	     

3. Click the HTML () icon on the scan job that you want to see.

The HTML report appears on the same page.

Vulnerabilities Found - 50

SUMMARY OF SCANNED HOSTS

HOST	HOSTNAME	Critical	High	Medium	Low	Info
192.168.73.111	VirtualUSMAllInOne	-	-	1	-	49

View false positives Additional information is available

192.168.73.111 - VirtualUSMAllInOne

REPORTED PORTS	
22/tcp	80/tcp
443/tcp	514/tcp
3128/tcp	3306/tcp
4369/tcp	9390/tcp

VULN NAME	VULNID	SERVICE	SEVERITY
Apache /server-status accessible	10677	https (443/tcp)	Medium ■■■■

Vulnerability Detection Result:
Vulnerable url: <https://VirtualUSMAllInOne.alienvault/server-status>
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
Summary:
Requesting the URI /server-status provides information on the server activity and performance.
Affected Software/OS:
All Apache installations with an enabled 'mod_status' module.
Impact:
Requesting the URI /server-status gives throughout information about the currently running Apache to an attacker.
Insight:
server-status is a Apache HTTP Server handler provided by the 'mod_status' module and used to retrieve the server's activity and performance.
Vulnerability Detection Method:
Checks if the /server-status page of Apache is accessible.
Solution:
- If this feature is unused commenting out the appropriate section in the web servers configuration is recommended.
- If this feature is used restricting access to trusted clients is recommended.
References:
https://httpd.apache.org/docs/current/mod/mod_status.html
CVSS Base Score: 5.0

Family name: Web application abuses
Category: infos
Created: 2005-11-03T13:08:04Z
Modified: 2020-12-01T08:30:14Z
CVEs: CVE-2020-25073

HTML report elements

Element	Definition																				
Scan Time	Time in which the report was made. It has the following format: yyyy-mm-dd hh:mm:ss.																				
Profile	Profile name that was chosen when the job was created.																				
Generated	Time it took to generate the report, in the format: yyyy-mm-dd hh:mm:ss.																				
Job Name	Name given to the job.																				
Chart Pie	A pie chart that displays all found vulnerabilities by severity, in percentages and in colors.																				
Summary of scanned hosts	<p>It displays the following table:</p> <table border="1"> <thead> <tr> <th colspan="6">SUMMARY OF SCANNED HOSTS</th> </tr> <tr> <th>HOST</th> <th>HOSTNAME</th> <th>Critical <input checked="" type="checkbox"/></th> <th>High <input checked="" type="checkbox"/></th> <th>Medium <input checked="" type="checkbox"/></th> <th>Low <input checked="" type="checkbox"/></th> <th>Info <input checked="" type="checkbox"/></th> </tr> </thead> <tbody> <tr> <td>192.168.73.111</td> <td>VirtualUSMAllInOne</td> <td>-</td> <td>-</td> <td>1</td> <td>-</td> <td>49</td> </tr> </tbody> </table> <p>Select the checkbox to enable the risk level view.</p>	SUMMARY OF SCANNED HOSTS						HOST	HOSTNAME	Critical <input checked="" type="checkbox"/>	High <input checked="" type="checkbox"/>	Medium <input checked="" type="checkbox"/>	Low <input checked="" type="checkbox"/>	Info <input checked="" type="checkbox"/>	192.168.73.111	VirtualUSMAllInOne	-	-	1	-	49
SUMMARY OF SCANNED HOSTS																					
HOST	HOSTNAME	Critical <input checked="" type="checkbox"/>	High <input checked="" type="checkbox"/>	Medium <input checked="" type="checkbox"/>	Low <input checked="" type="checkbox"/>	Info <input checked="" type="checkbox"/>															
192.168.73.111	VirtualUSMAllInOne	-	-	1	-	49															
Vulnerability Details	<p>This table includes the vulnerability name, the vulnerability ID, the service name, and the severity of that vulnerability.</p> <p>The background color refers to the type of vulnerability: pink = Critical, salmon = High, gold = Medium, yellow = Low, and light pale yellow = Info.</p>																				

Viewing the Scan Results in PDF

When you export a report in a PDF file, you can see a logo and the name of the portal branding. This information is configured through the Settings option.

To view the scan results in PDF

1. Go to **Environment > Vulnerabilities > Overview**.
2. Click **Report History** if that part has not been expanded.
3. Click the PDF () icon on the scan job that you are interested in.

The report in PDF format opens in a new tab.

To change the site header logo and the portal branding in a PDF

1. Go to **Environment > Vulnerabilities > Overview**, click **Settings**.
2. In the **Site header logo** field, type the path and name of the header logo file you want to use.
3. In the **Portal Branding** field, type the company name you want appear on the report.
4. Click **Update**.
5. Close the window by clicking the close icon (✕).

Viewing the Scan Results in Excel

When you export a report in an Excel file, you can see the name of the portal branding. This information is configured through the **Settings** option.

To view the scan results in Excel

1. Go to **Environment > Vulnerabilities > Overview**.
2. Click **Report History** if that section has not been expanded.
3. Click the Excel () icon on the scan job that you want to export.
4. Depending on the browser, a new popup may appear asking if you want to open the file or save it; or your browser downloads the file directly.

The name of the Excel file has the following structure: `ScanResult_YYYYMMDD_.xls`.

To change the portal branding in an Excel file

1. Go to **Environment > Vulnerabilities > Overview**, click **Settings**.
2. In the **Portal Branding** field, type the company name you want appear on the report.
3. Click **Update**.
4. Close the window by clicking the close icon (✕).

Importing Scan Results

This option allows you to import results from external scanners to create reports or perform cross-correlation.

To import a scan result file

1. Go to **Environment > Vulnerabilities > Scan Jobs**.
2. Click **Import AlienVault Scan**.

3. Enter a name for the report.
4. Select the file to import.



Note: Starting from USM Appliance version 5.8.7, you can only import scan files produced by another instance of USM Appliance and exported in an NBE file. Importing of other types of scan results is no longer supported.

5. In the Assign to list, select a single user or an entity.

The chosen user or entity becomes the owner of the scan in the USM Appliance.

6. To import the vulnerabilities and add the new assets, click **Import & Asset Insertion**.

To import the vulnerabilities only, click **Import**.

A message appears to inform you that the file has been imported successfully.

7. Close the window by clicking the icon.

Comparing the Results from Two Scans

The USM Appliance web interface can display a comparison of the results in both text and graphical format from two previous scans.

To compare two reports

1. Go to **Environment > Vulnerabilities > Overview**.
2. Click **Reports** if that section has not been expanded.
3. To select a report for comparison, click its spreadsheet (📄) icon.

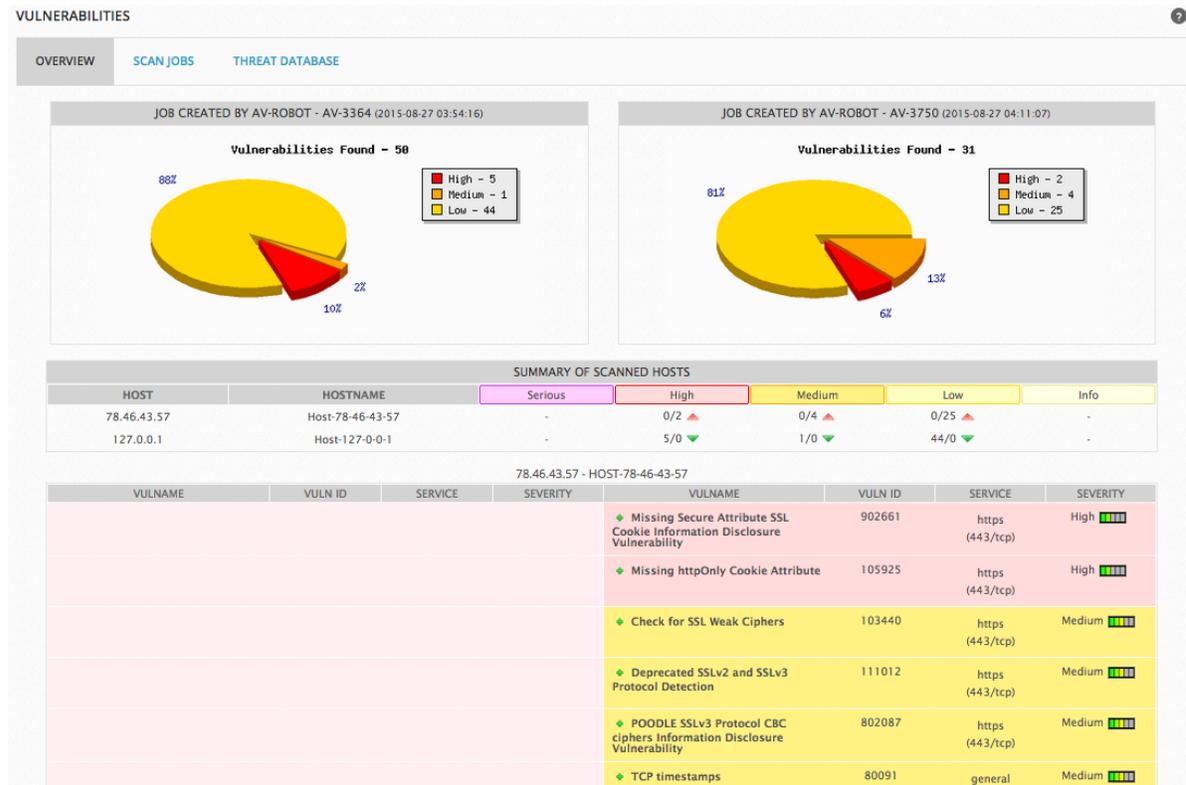
The Compare Reports window appears.



4. Select the second report from the **Second report** list.
5. Click **Compare**.

USM Appliance tries to match the vulnerabilities in the two reports displays them side-by-

side, similar to below:



Vulnerability Scan Profiles

When performing scans, you must select a scanning profile. Using a set of network vulnerability tests (NVTs) organized by families, each profile determines the type of scan to perform and how thorough the scan should be.

In USM Appliance, go to **Environment > Vulnerabilities > Overview** and then click **Profiles** to see the list of scan profiles. You can't view, modify, or delete the built-in scan profiles, but you can [create new profiles](#) by cloning the existing ones. You can view the cloned profiles and see what plugins are included in each profile. You can [modify or delete](#) any profile you created.

Starting from version 5.8.7, USM Appliance provides the following scan profiles for you to choose from:

Profiles



VULNERABILITY SCAN PROFILES			
AVAILABLE FOR	PROFILE	DESCRIPTION	ACTION
All	Base	Basic configuration template with a minimum set of NVTs required for a scan.	
All	Discovery	Network Discovery scan configuration.	
All	empty	Empty and static configuration template.	
All	Full and fast	Most NVT's; optimized by using previously collected information.	
All	Full and fast ultimate	Most NVT's including those that can stop services/hosts; optimized by using previously collected information.	
All	Full and very deep	Most NVT's; don't trust previously collected information; slow.	
All	Full and very deep ultimate	Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.	
All	Host Discovery	Network Host Discovery scan configuration.	
All	System Discovery	Network System Discovery scan configuration.	

[CREATE NEW PROFILE](#)

Vulnerability Scan Profiles in USM Appliance Version 5.8.7 and Later

Profile Name	Description
Base	<p>This scan profile contains NVTs that collect information about the target systems. It uses <i>Ping</i> and <i>Nmap</i> to detect if a host is alive and collects information about the operating system (OS). It doesn't detect vulnerabilities.</p> <p>The NVT families are static. After the profile is created, the set of NVTs stays the same.</p>
Discovery	<p>This scan profile contains NVTs that provide information about the target systems. It collects information about open ports, used hardware, firewalls, installed software and certificates, and used services. It doesn't detect vulnerabilities.</p> <p>The NVT families are dynamic. After the profile is created, new NVTs in the selected NVT families are added and used automatically.</p>
Empty	<p>This scan profile contains no NVT. You can clone it and create a scan profile from scratch.</p>

Vulnerability Scan Profiles in USM Appliance Version 5.8.7 and Later(Continued)

Profile Name	Description
Full and fast	<p>This scan profile contains NVTs that won't damage the target systems. It conducts a port scan to gather information about the system first and use the relevant NVTs based on the information collected to complete the scan. These NVTs are optimized to keep the false negative rate low.</p> <p>The NVT families are dynamic. After the profile is created, new NVTs in the selected NVT families are added and used automatically.</p>
Full and fast ultimate	<p>This scan profile expands the <i>Full and fast</i> profile with NVTs that could disrupt services or systems, or even cause shutdowns. It conducts a port scan to gather information about the system first and use the relevant NVTs based on the information collected to complete the scan. These NVTs are optimized to keep the false negative rate low.</p> <p>The NVT families are dynamic. After the profile is created, new NVTs in the selected NVT families are added and used automatically.</p>
Full and very deep	<p>This scan profile is based on the <i>Full and fast</i> profile but without taking into account the result of the port scan. In other words, it includes NVTs that wait for a timeout and NVTs that test vulnerabilities of an application that wasn't detected, making the scan very slow.</p> <p>The NVT families are dynamic. After the profile is created, new NVTs in the selected NVT families are added and used automatically.</p>
Full and very deep ultimate	<p>This scan profile expands the <i>Full and very deep</i> profile with NVTs that could disrupt services or systems, or even cause shutdowns. The scan is very slow.</p> <p>The NVT families are dynamic. After the profile is created, new NVTs in the selected NVT families are added and used automatically.</p>
Aggressive	<p>This scan profile runs all vulnerability-related scripts regardless of whether they are safe for the scanned target.</p> <p>This can cause a significant performance drop as well as issues such as Denial of Service (DoS), malfunctions, and errors.</p>

Vulnerability Scan Profiles in USM Appliance Version 5.8.7 and Later(Continued)

Profile Name	Description
Host discovery	<p>This scan profile contains NVTs that use <i>Ping</i> to detect if a host is alive. It doesn't detect vulnerabilities.</p> <p>The NVT families are static. After the profile is created, the set of NVTs stays the same.</p>
System discovery	<p>This scan profile contains NVTs that use <i>Ping</i> to detect if a host is alive and <i>Nmap</i> to collect information about the OS and hardware. It doesn't detect vulnerabilities.</p> <p>The NVT families are static. After the profile is created, the set of NVTs stays the same.</p>



Note: USM Appliance version 5.8.6 and earlier only has three scan profiles:

- **Deep:** A non-destructive full and slow scan.
- **Default:** A non-destructive full and fast scan. Use this profile if the target system tends to break or crash with the scanning requests.
- **Ultimate:** A full and fast scan including destructive tests. It includes stress tests that can crash the target system. For example, filling a network switch with random MAC addresses.

Creating a Custom Scan Profile

You can create a custom profile and tailor it to the type of the target system you are scanning.

To create a custom profile for vulnerability scans

1. Go to **Environment > Vulnerabilities > Overview**.
2. Click **Profiles**, and then click **Create New Profile**.

Profiles ✕

NEW PROFILE

Name:

Description:

Clone existing scan policy:

Make this profile available for User: OR Entity:

Autoenable plugins by family:

FAMILY	<input type="checkbox"/> ENABLE ALL	<input type="checkbox"/> ENABLE NEW	<input type="checkbox"/> DISABLE ALL
AIX Local Security Checks	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Amazon Linux Local Security Checks	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brute force attacks	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Buffer overflow	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CentOS Local Security Checks	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
CISCO	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Citrix Xenserver Local Security Checks	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. Fill in the following details:

- **Name** — The name for your scan profile. You will use it later to select from drop-down menus during vulnerability scan setup.
- **Description** — The description of the scan profile.
- **Clone existing scan policy** — Allows you to select an existing profile to use as a template for the new profile.
- **Make this profile available for** — Designate who will have access to the profile. You can select a single user, allow all users to access it, or select an organizational entity to allow access to all users within that entity to access the profile.
- **Autoenable plugins by family** — Select the plugins you want to enable for this profile.



Note: Auto-enable plugins by category has been deprecated in USM Appliance version 5.8.7 and later.

4. Enable or disable the plugins as needed with the **Enable All** or **Disable All** options. Currently, the **Enable New**, **Disable New**, and **Intelligent** options have no designated functionality in USM Appliance.

- Click **Create** after you have finished your selection.

USM Appliance displays "Update Status" at the top of the page.

After it finishes creating the new profile, the vulnerabilities overview page displays.

- Click **Profiles** to see the created profile.

Modifying a Custom Scan Profile

To modify a custom profile for vulnerability scans

- Go to **Environment > Vulnerabilities > Overview**, and click **Profiles**.
- Click the pencil () icon of the profile you want to modify.

The **Edit Profile: <name of profile>** popup displays.

Profiles ✕

EDIT PROFILE: COPY OF FULL AND FAST

EDIT EDIT PLUGINS EDIT PREFS VIEW CONFIG

NAME:

DESCRIPTION:

MAKE THIS PROFILE AVAILABLE FOR: User: OR Entity:

AUTOENABLE OPTIONS BY FAMILY:

FAMILY	<input type="checkbox"/> ENABLE ALL	<input type="checkbox"/> ENABLE NEW	<input type="checkbox"/> DISABLE ALL
AIX Local Security Checks	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Amazon Linux Local Security Checks	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Brute force attacks	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Buffer overflow	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
CentOS Local Security Checks	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
CISCO	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Citrix XenServer Local Security Checks	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>



Note: Only admin and global admin accounts can modify a custom profile. Non-admin users can only edit the profiles they've created. USM Appliance built-in scan profiles can't be modified.

- Modify the settings as needed.

Options available in a custom profile

Option	Description
Edit	Allows users to modify the name, description, owner, and the auto-enable families for the profile.
Edit Plugins	Allows for detailed adjustment of the plugins that the AlienVault vulnerability scanner uses to scan your assets. USM Appliance displays the number of plugins available as well as the number of plugins enabled in the current profile.
Edit Prefs	Allows for personalized configuration for each profile. These preferences are generated dynamically. They may change after an AlienVault Lab Intelligence Update.
View Config	Shows the final configuration. USM Appliance displays the preferences selected in the previous option in plain text.

4. Click **Update**.

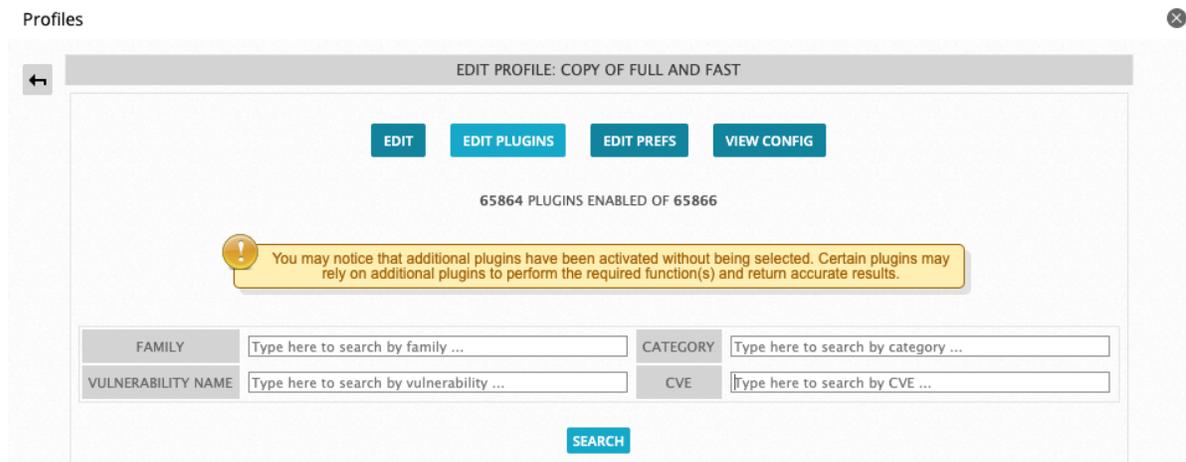
USM Appliance displays "Update Status" at the top of the page.

After it completes, the vulnerabilities overview page displays.

To enable or disable specific plugins

1. Click **Edit Plugins** when editing a profile.

USM Appliance displays the list of plugins with search options: Family, Category, Vulnerability Name, and CVE.



- Use one of the options to search, depending on what you are looking for.

USM Appliance displays the list of plugins based on your selection.

The screenshot shows a search interface with the following search criteria:

- FAMILY: Type here to search by family ...
- VULNERABILITY NAME: Type here to search by vulnerability ...
- CATEGORY: Type here to search by category ...
- CVE: CVE-2018-7356

The search results table is as follows:

VULNERABILITY ID	VULNERABILITY NAME	CVE ID	PLUGIN FAMILY	PLUGIN CATEGORY
<input checked="" type="checkbox"/> 103701	TCP/IP Predictable TCP Initial Sequence Number Vulnerability	CVE-1999-0077 CVE-2000-0328 CVE-2000-0916 CVE-2001-0162 CVE-2001-0288 CVE-2001-0328 CVE-2002-1463 CVE-2003-1230 CVE-2004-0641 CVE-2007-2782 CVE-2015-3963 CVE-2018-7356	Buffer overflow	infos

Showing 1 to 10 of 168 plugins. Navigation: FIRST PREVIOUS 1 2 3 4 5 NEXT LAST. A 'SAVE' button is at the bottom.

- Select the plugins you want to enable or disable, and then click **Save**.
- Alternatively, use the **Search Actions > Enable All/Disable All** buttons to enable or disable all the plugins belonging to the same group.

To search the Threat Database for available plugins

- Go to **Environment > Vulnerabilities > Threat Database**.

USM Appliance displays the threat families with the number of plugins in each severity.

The Threat Database interface shows the following table:

THREAT FAMILY	INFO	LOW	MEDIUM	HIGH	TOTAL
General	18,396	48,944	444,220	472,444	984,004
Credentials	734	0	0	0	734
Malware	4	0	6	44	54
Citrix XenServer Local Security Checks	0	1	8	21	30
RPC	170	0	4	4	178
Web Servers	6	23	459	120	608

2. Use one of the four methods, **Date Range**, **Keywords**, **CVE ID**, and **Risk Factor**, to search for the plugin you want.
3. Click **Search**.

This returns a list of the plugins related to the search. Hovering the mouse over an ID will display the plugin details.

VULNERABILITIES

OVERVIEW SCAN JOBS THREAT DATABASE

SEARCH RESULTS FOR THIS CRITERIA

START DATE	END DATE	KEYWORDS	CVE ID	FAMILY	RISK FACTOR
All	All	All	CVE-2014-4863	All	All

ID	RISK	CREATED ON	THREAT FAMILY & SUMMARY	CVE ID
10264		2014-03-12T09:10:24Z	SNMP - Simple Network Management Protocol (SNMP) is a protocol which can be used by administrators to remotely manage a computer or network device. There are typically 2 modes of remote SNMP monitoring. These modes are roughly 'READ' and 'WRITE' (or PUBLIC)	CVE-1999-0472 CVE-1999-0516 CVE-1999-0517 CVE-1999-0792 CVE-2000-0147 CVE-2001-0380 CVE-2001-0514 CVE-2001-1210 CVE-2002-0109 CVE-2002-0478 CVE-2002-1229 CVE-2004-1474 CVE-2004-1775 CVE-2004-1776 CVE-2011-0890 CVE-2012-4964 CVE-2014-4862 CVE-2014-4863 CVE-2016-1452 CVE-2016-5645 CVE-2017-7922 CVE-2020-5364
105072		2014-08-25T11:47:33Z	SNMP - The remote ARRIS DOCSIS is prone to a security-bypass vulnerability.	CVE-2014-4863

Note: The CVE links take you to the corresponding Vulnerability Details page on <http://www.cvedetails.com>.

Changing the Vulnerability Ticket Threshold

As discussed in the [Vulnerability Risk Factors](#), USM Appliance sets a threshold for vulnerabilities and generates a ticket automatically whenever the detected vulnerability surpasses the threshold.

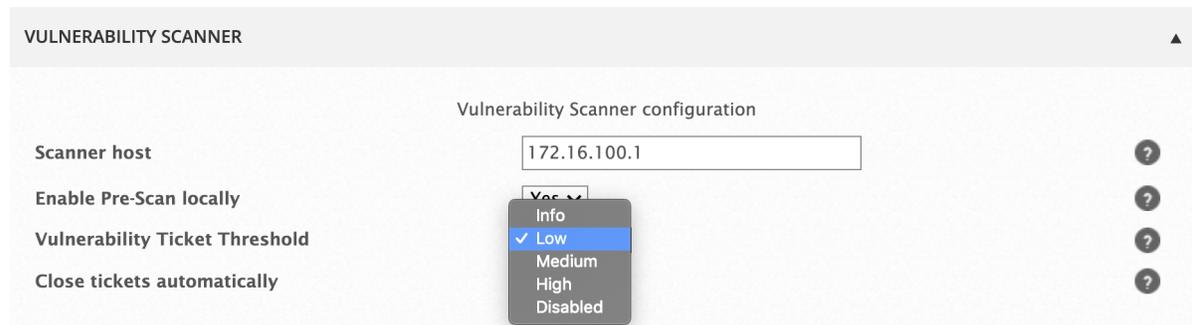
The values of the Vulnerability Ticket Threshold field are **Info**, **Low**, **Medium**, **High**, and **Disabled**. The default value is Low, but this is user-configurable. If you set the threshold to Disabled, USM Appliance will not open any ticket when it detects a vulnerability.

You can change the threshold from the following locations:

- Configuration > Administration > Main > Vulnerability Scanner
- Environment > Vulnerabilities > Overview > Settings

To change the vulnerability threshold setting from Configuration

1. Go to **Configuration > Administration > Main > Vulnerability Scanner**.



2. Select a value from the **Vulnerability Ticket Threshold** list.
3. To save the change, click **Update Configuration**.

To change the vulnerability ticket threshold from Environment

1. Go to **Environment > Vulnerabilities > Overview > Settings**.
2. From the **Settings** dialog box, select the appropriate threshold value from the **Vulnerability Ticket Threshold** list.

SETTINGS

Site header logo:	<input style="width: 90%;" type="text" value="../pixmaps/logo_siempdf.png"/>
Portal Branding:	<input style="width: 90%;" type="text" value="AlienVault"/>
Vulnerability Ticket Threshold:	<div style="border: 1px solid #ccc; background-color: #333; color: #fff; padding: 5px; width: fit-content;"><ul style="list-style-type: none">Info<li style="background-color: #0070c0; color: #fff;">✓ LowMediumHighDisabled</div>
Close Tickets Automatically:	

3. Click **Update**.

Changing Other Vulnerability Scanner Options

You can modify the default vulnerability scanner settings to optimize the scanner for your environment. For example, you can change the default port number (9390) for the vulnerability scanner if this port is already in use.

To change the vulnerability scanner configuration

1. Go to **Configuration > Administration > Main**.
2. Click **Vulnerability Scanner** to display the fields underneath.

3. Change any of the fields as needed.

Field descriptions for the AlienVault Vulnerability Scanner

Field	Description
Scanner host	The IP address that identifies the host (only for non-distributed scans)
Enable Pre-Scan locally	Only performs the pre-scan if the USM Appliance Sensor is local, such as in a USM Appliance All-in-One. The default value is No.
Vulnerability Ticket threshold	Choose a value between Info, Low, Medium, High and Disabled. The default value is Low. See Changing the Vulnerability Ticket Threshold for details.
Close tickets automatically	When enabled, tickets related to vulnerabilities will be automatically closed if the vulnerabilities found in the previous scans are not present in the latest scan.

4. Click **Update Configuration**.

By default, USM Appliance can run five vulnerability scans simultaneously per USM Appliance Sensor. If you configure a new scan job when there are already 5 scans running on the same USM Appliance Sensor, USM Appliance delays the job to for 15 minutes. Should the USM Appliance Sensor has not finished scanning at that time, USM Appliance delays the job for another 15 minutes, until the USM Appliance Sensor is available to start the new scan.

To lower the maximum number of simultaneous scans

1. Go to **Configuration > Deployment > Components > Sensors**.
2. Double-click the USM Appliance Sensor you want to change.

The configuration options for the USM Appliance Sensor display.

Values marked with () are mandatory*

NAME *	<input type="text" value="VirtualUSMAllInOne"/>
IP *	<input type="text" value="192.168.73.111"/>
PRIORITY	<input type="text" value="5"/>
TIMEZONE	<input type="text" value="GMT-4:00"/>
DESCRIPTION	<input type="text"/>

SAVE

INVENTORY TASK

NAME	TASK TYPE	FREQUENCY	ACTION
<input type="text"/>	<input type="text" value="Asset Discovery Scan"/>	<input type="text" value="Hourly"/>	NEW TASK

PARAMETERS

ADVANCED OPTIONS

Scan type:

Timing template:

Autodetect services and Operating System

Enable reverse DNS Resolution

SERVICES

VULNERABILITY ASSESSMENT CONFIGURATION	ACTION
Max Simultaneous Scans: <input type="text" value="5"/>	UPDATE

3. Drag the bar to adjust a value between 1 to 5.
4. Click **Update**.

Open Threat Exchange® and USM Appliance

When you sign up for and connect your Open Threat Exchange® (OTX™) account to your USM Appliance instance, it configures USM Appliance to receive raw pulse data.

This section covers the following subtopics:

What is Open Threat Exchange®?	356
Using OTX in USM Appliance	359

What is Open Threat Exchange®?

Open Threat Exchange®(OTX™) is a threat data platform that allows security researchers and threat data producers to share research and investigate new threats.

OTX provides open access for all, allowing you to collaborate with a worldwide community of threat researchers and security professionals. This access enables collaborative research by allowing everyone in the OTX community to actively share threat data, trends, and techniques.

In addition to accelerating the distribution of the latest threat data, OTX automates the process of updating your security infrastructure. By offering a platform for the community of security analysts to actively collaborate, OTX strengthens the defenses of all who use it.

Information in OTX derives from both public and private entities, as well as other resources.

The OTX platform consists of two chief components:

- **Pulses**

Collections of indicators of compromise (IoCs), reported by the OTX community, which other community members review and comment on. Pulses provide you with a summary of the threat, a view into the software targeted, and the related IoCs, reported by the OTX community worldwide. See [OTX Pulses and Indicators of Compromise](#).

- **IP Reputation**

Provides notification of communication between known malicious hosts and your assets. See [OTX IP Reputation](#).

OTX Pulses and Indicators of Compromise

The OTX community reports on and receives threat data in the form of “pulses.” A pulse consists of at least one, but more often multiple Indicators of Compromise (IoCs).

An IoC is an artifact observed on a network or in an end point judged with a high degree of confidence to be a threat vector. Examples of threat vectors include campaigns or infrastructures used by an attacker. The following table provides a list of IoC types.

Indicator of compromise (IoC) types

IoC Type	Description
CIDR	Classless inter-domain routing. Specifies a range of IP addresses on a network that is suspected of malicious activity or attack.
CVE	Standards group identification of Common Vulnerabilities and Exposures (CVEs).
domain	A domain name for a website or server suspected of hosting or engaging in malicious activity. Domains may also encompass a series of hostnames.
email	An email address associated with malicious activity.
FileHash (MD5, SHA1, SHA256, PEHASH, IMPHASH)	A hash computation for a file that can be used to determine whether contents of a file may have been altered or corrupted.
filepath	Unique location in a file system of a resource suspected of malicious activity.
hostname	The hostname for a server located within a domain, suspected of malicious activity.
filepath	Unique location in a file system of a resource suspected of malicious activity.
IPv4, IPv6	An IP address used as the source/destination for an online server or other device suspected of malicious activity.
Mutex	Mutual exclusion object allowing multiple program threads to share the same resource. Mutexes are often used by malware as a mechanism to detect whether a system has already been infected.
FileHash-SHA256	A SHA256-format hash that summarizes the architecture and content of a file deemed suspicious.
URI	A uniform resource identifier (URI) that describes the explicit path to a file hosted online, which is suspected of malicious activity.
URL	Uniform resource locations (URLs) that summarizes the online location of a file or resource associated with suspected malicious activity.

OTX IP Reputation

OTX IP Reputation identifies IP addresses and domains worldwide that are submitted by the OTX community. IP Reputation verifies them as either malicious or, at least, suspicious until more data comes in to increase their threat ranking. Through its incoming IP data from all of these sources, IP Reputation supplements OTX data with valuable data about actively or potentially malicious activity appearing worldwide that can affect your system.

IP Reputation Data Sources

IP Reputation receives data from a variety sources

- Hacker forums
- Open-source intelligence — Public and private security research organizations.
- USM Appliance/AlienVault OSSIM® deployments—Consists of users who have voluntarily agreed to anonymously share information about external traffic into their network with AlienVault.



Note: AlienVault ensures that none of the data shared with OTX can be traced to the contributor or their USM Appliance instance.

Who Has Access to IP Reputation?

All USM Appliance users receive the benefit of IP Reputation data whether or not they sign up for an OTX account.

When you open an OTX account, you may elect to share IP Reputation data with other OTX users. Any data you contribute are anonymous and secure.



Note: You can configure USM Appliance to stop sharing IP Reputation data with OTX at any time by visiting the **Open Threat Exchange Configuration** page.

IP Reputation Ranking Criteria

IP Reputation uses ranking criteria based on IP Reliability and IP Priority that OTX updates on an ongoing basis to calculate changing assessments to risk level. This helps prevent false positives.

IP Reliability

IP Reputation data derives from many data sources of differing reliability. Ranking in this case is based on the relative number of reports regarding a malicious IP in relation to others reported. If, for example, OTX receives 10 reports on a given IP address versus 20 on another, it gives the IP with 10 reports a lower reliability ranking than the IP with 20 reports.

IP Priority

OTX ranks IP address priority, based on the behavior associated with each IP address listed. For example, an IP address used as a scanning host receives a lower priority than an IP address known to have been used as a Botnet server.

Ongoing Ranking Reassessment

OTX constantly updates its IP Reputation data as new information emerges affecting IP reliability or priority criteria. Each update reprioritizes IP reliability and priority values and the threat level of an IP accordingly.

Using OTX in USM Appliance

When you sign up for and connect your Open Threat Exchange® (OTX™) account to your USM Appliance instance, it configures USM Appliance to receive raw pulse data and other IP reputation information.



Note: Reputation data is updated separately from OTX pulse information.

USM Appliance then correlates that data with incoming events, alerting you to OTX pulse and IP Reputation-related security events/alarms when it detects IoCs interacting with assets in your environment. Such interactions might consist of malicious IPs communicating with systems, malware detected in your network, or outbound communication with command-and-control (C&C) servers.

Connecting OTX to USM Appliance helps manage risks and threats in the following ways:

- USM Appliance detects threat updates every 30 minutes for all pulses to which you subscribe, either directly or through subscriptions to other OTX users.
- You receive updates on your subscribed pulses by email, either individually as they occur or in digest mode.
- You can review OTX pulses about related threat vectors in USM Appliance.

- As soon as you log into USM Appliance, you can see which pulses are most active in your environment by looking at the USM Appliance Dashboards Overview.
- USM Appliance checks OTX pulses against all NIDS events. It generates an alarm when a malicious IP address communicates with any of your assets, or when some of the other IoCs, including CIDR (IPv4 only), domain, and hostname, are detected in your network.
- In a distributed environment, the USM Appliance Server replicates the OTX pulses to the connected USM Appliance Sensors through TCP port 6380. This replication is read-only so that the copy on the USM Appliance Server remains intact.



Note: When a USM Appliance Sensor is added to the USM Appliance Server, a firewall rule is created to allow OTX traffic going through TCP port 6380. When the Sensor is removed, the firewall rule is deleted. The same mechanism is used in a high availability (HA) deployment to replicate OTX pulses between nodes.

Following sections describe collection of IP Reputation information used in calculating risk for specific events. In addition, information is provided on filtering events based on related pulse information and risk based on specific IP Reputation levels.

OTX IP Reputation Data Correlated with Events

USM Appliance maintains an IP reputation list that stores data it receives from OTX about public IP addresses involved in malicious or other suspect activities. Whenever an event has its source or destination IP addresses listed in the IP Reputation list, reputation data will be added to the data stored for the event. This allows USM Appliance to support some additional features like reprioritization of events and alarms depending on the IP of the hosts involved.

The IP reputation list maintained by USM Appliance is stored on the USM Appliance Server in the `/etc/ossim/server/reputation.data` file. Activity, Reliability, and Priority values provided by OTX are saved with event information for those events having reputation data for either source or destination IP addresses.

The main purpose of the IP reputation list is to provide a list of known or potentially dangerous IP addresses. If any alarm or event is generated by the action of a listed dangerous IP address, then this event will have a smaller probability of being a false positive. This also allows for the recalculation of event/alarm risk depending on its "IP Reliability" and "IP Priority" values.



Note: Reputation events are anonymized and submitted to the AlienVault OTX service for those customers who enable that capability in USM Appliance. With the feedback received from customer systems and all the other sources AlienVault uses, the IP Reputation values are updated before being redistributed to customers.

Displaying Alarms and Events Based on OTX Pulse and IP Reputation

The USM Appliance Alarm and Security Events (SIEM) web UI each provide methods of searching for and filtering alarm and security events based on OTX pulse and IP Reputation information. For each event, the database stores associated information on the source and destination IP address provided by OTX, in addition to the activity reported in the event, for example, spamming, phishing, scanning, malware distribution, and so on.

Viewing OTX Alarms

Different from the way other alarms are processed, USM Appliance generates an alarm whenever it detects even *one event* associated with an OTX pulse. Alarm correlation begins at that point and proceeds for a period of 24 hours. During this time, USM Appliance adds any new events related to that pulse to the same alarm.

If any new events related to the pulse occur after that 24-hour period, USM Appliance generates a second alarm and a new correlation period begins. As an exception to this rule, should an event contain data on record with OTX IP Reputation information, USM Appliance correlates the alarm, using its standard directive taxonomy.



Note: If an OTX pulse is creating too much noise and generating too many false positive alarms, you can always just unsubscribe from the pulse.

USM Appliance does not offer a filter for IP Reputation-based alarms. However, you can view these within the Alarms list, where they occur.

Searching, Filtering, and Viewing Events

From the USM Appliance Security Events (SIEM) page, you can search for and filter events based on whether OTX pulses exist for source or destination IP addresses, as well as the severity of different IP Reputation scores. The following screen shot highlights fields in which you can select OTX pulse and IP Reputation search/filter options.

SECURITY EVENTS (SIEM)

SIEM
REAL-TIME
EXTERNAL DATABASES

GO
?

SHOW EVENTS

Last Day

Last Week

Last Month

Date Range

📅

-

📅

like

DATA SOURCES

DATA SOURCE GROUPS

SENSORS EXCLUDE

ASSET GROUPS

NETWORK GROUPS

RISK

OTX IP REPUTATION

OTX PULSE

Pulse name

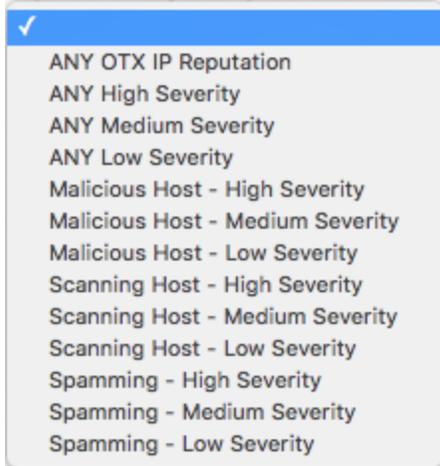
ONLY OTX PULSE ACTIVITY

CLEAR FILTERS
↻

Last Day ✕

ADVANCED SEARCH

Selecting the OTX IP Reputation field opens a menu list in which you can choose to display only events that meet or exceed a specific IP Reputation severity level.



The Low, Medium, and High severity levels take in account the OTX IP priority values of both the source and destination IP addresses included in events, based on the following rules:

- **Low Severity** — returns events that have a source or destination IP priority of 0, 1, or 2.
- **Medium Severity** — returns events that have a source or destination IP priority of 3, 4, 5, or 6.
- **High Severity** — returns events that have a source or destination IP priority greater than 6.

Once you've made your selection, the Event list display will be updated to show only those events matching the IP Reputation criteria you specified, plus OTX pulse information, if you selected that option.

<input type="checkbox"/>	EVENT NAME	▼ DATE GMT-4:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	RISK
<input type="checkbox"/>	URL URL URL URL URL AlienVault NIDS: "ET SCAN NMAP"	2017-09-14 18:55:34	stable		106.75.90.187:58914	stable:80	LOW (0)
<input type="checkbox"/>	directive_alert: Unknown event	2017-09-14 18:55:34	N/A		106.75.90.187:58914	stable:80	MED (1)
<input type="checkbox"/>	directive_alert: Unknown event	2017-09-14 14:43:18	N/A		191.96.249.136:53070	stable:80	MED (1)
<input type="checkbox"/>	URL URL URL URL URL AlienVault NIDS: "ET SCAN NMAP"	2017-09-14 14:43:18	stable		191.96.249.136:53070	stable:80	LOW (0)

In this example, the event list display shows events in which the **Any OTX IP Reputation** filter option was selected. The OTX field displays the blue  icon, indicating the event has OTX IP Reputation information. (An orange icon is displayed when OTX has pulse information for the event.)

Displaying OTX Pulse and IP Reputation Information in Event and Alarm Displays

In the **SIEM Events** list, you can click the orange or blue OTX  icon to display the OTX IP Reputation information available for an event, as shown below.

OTX DETAILS

OTX IP Reputation				
TYPE	INDICATOR	ACTIVITY	RELIABILITY	PRIORITY
Source	93.174.93.203	Scanning Host	2	2

Go to OTX to get more information. 

SHOWING 1 TO 1 OF 1 INDICATORS FIRST PREVIOUS 1 NEXT LAST

OTX Details — IP Reputation

Field	Description
Type	Tells you whether the indicator is the source or the destination of the event.
Indicator	IP address or hostname of the event source.
Activity	Type of malicious activity identified, for example, a scanning host.
Reliability	OTX IP reliability score, with values ranging from 1 to 10; 10 being the highest reliability.
Priority	OTX IP priority score, with values ranging from 1 to 10; 10 being the highest priority.
Magnifying glass icon	Clicking on the magnifying glass icon takes you to OTX to learn more about the indicator.

From the SIEM Events list display, you can also click the magnifying glass icon to display additional event details, plus OTX and risk information.

SECURITY EVENTS (SIEM)

SIEM

REAL-TIME

EXTERNAL DATABASES

[Security Events](#) > *AlienVault NIDS: "ET SCAN NMAP -sS window 1024"*

AlienVault NIDS: "ET SCAN NMAP -sS window 1024" ACTIONS ▾

DATE	2017-09-21 06:38:20 GMT-4:00	CATEGORY	Recon
ALIENVAULT SENSOR	devel [172.16.100.1]	SUB-CATEGORY	Misc
DEVICE IP	172.16.100.1 [eth0]	DATA SOURCE NAME	AlienVault NIDS
EVENT TYPE ID	2009582	DATA SOURCE ID	1001
UNIQUE EVENT ID#	9eb811e7-a75a-000c-2931-6aeffc4dd43c	PRODUCT TYPE	Intrusion Detection
PROTOCOL	TCP	ADDITIONAL INFO	URL URL URL URL URL

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
2	1	LOW (0)	1

From this display, you can click the number in blue under OTX Indicators to get more OTX details about an indicator.

In addition to other navigation options, in both Alarm and SIEM Event list views, you can right-click on Source and Destination IP addresses or host names, which will display a popup menu of available actions you can take corresponding to a specific IP address or host name.

<input type="checkbox"/>	EVENT NAME	▼ DATE GMT-4:00 ▲	SENSOR	OTX	SOURCE	DESTINATION	RISK
<input type="checkbox"/>	AllenVault HIDS: Login session opened.	2017-05-31 09:27:19	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: Login session closed.	2017-05-31 09:27:19	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: USB device added/removed	2017-05-31 09:25:01	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: USB device added/removed	2017-05-31 09:25:01	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: Login session closed.	2017-05-31 09:24:49	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: Login session opened.	2017-05-31 09:24:47	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: Login session opened.	2017-05-31 09:24:47	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: Login session closed.	2017-05-31 09:24:47	devel	N/A	devel	devel	LOW (0)
<input type="checkbox"/>	AllenVault HIDS: Login session opened.	2017-05-31 09:24:45	devel	N/A	devel	devel	LOW (0)

- 📁 All events from this host
- 🔍 Events as source
- 🔍 Events as destination
- 📄 Stats and Info
- 🔍 Analyze Asset
- 🔍 Look up in OTX
- 📄 Asset Detail
- 🔧 Configure Asset
- 🌐 Whois
- 📄 Tickets
- 🔔 Alarms
- 📄 Log
- 🌿 Vulnerabilities
- 📄 Traffic
- 📄 Related Traffic
- 📄 Availability

For example, the **Look up in OTX** option opens the OTX site to display potential and reported threats related to the selected location. If no threat information is found about the location, the **Look Up in OTX** option opens the Create New Pulse web page in OTX, which lets you create a new Pulse to report a possible new threat.

Incident Response

Organizations are bombarded with potential threats every day. Most of the events or incidents posing threats are not likely to cause any damage in your environment, but they need to be investigated, nonetheless. To quickly and efficiently investigate and respond to threats, you need a plan. An incident response plan defines your response, not only to effectively address specific, individual incidents, but also to examine sequences of events to determine if they may match the steps an attacker might take to compromise security in your environment.

The ultimate goal of an incident response plan is not only to effectively address specific, single incidents, but also identify potential threats originating from a sequence of events or incidents that could be used to carry out a broader attack. Having a plan, complete with procedures and processes in place to address different scenarios is important, because, even if you accept that nothing will go exactly according to plan, it still will provide a valuable checklist and reference for everything that needs to be done. That can provide incredible value, especially during highly stressful times of crisis.

Many different security organizations and standards groups publish recommendations or guidelines for incident response processes for companies to follow for their network security incident investigation, remediation or mitigation, and follow-up. These recommendations typically include very similar elements such as the following:

- **Preparation** — Preparing IT and an incident response team of people with resources, procedures, priorities, and escalation to handle potential incidents in case they happen; deployment and monitoring setup to establish baseline behavior. Setting up alarms, eliminating false positives and false negatives.
- **Analysis, Detection, and Identification** — Developing tools and providing specific instructions and procedures to analyze incidents, analyze their severity, identify actual and potential exploits associated with incidents, and determining the priority and possible escalation in remediation or mitigation of threats and vulnerabilities.
- **Containment, Eradication, and Recovery** — Guidelines for isolating systems affected by security incidents, to prevent further damage, finding and eliminating the root cause of attacks, and remediating or mitigating threats. Permitting affected systems back into the production environment after addressing issues (and monitoring systems for future repeat incidents).

- Post-Incident Activity and Lessons Learned — post-mortem data collection and reporting following resolution of issues. Documenting activities and results in addressing incidents and maintaining records for compliance assessments. Review and discussion with all incident response team members, to improve future incident response efforts.

 **Note:** AlienVault's website provides a free downloadable PDF eBook, *AlienVault's Insider's Guide to Incident Response*, that includes many practical tips and advice for developing your own incident response plan, and directing your incident response team to investigate and address security incidents in your own environment.¹

What Defines an Incident?

An incident is an unplanned event that requires some measure of investment of time and resources to rectify. Eventually you are going to develop your own internal grading system for incidents, but this is the measure most organizations should begin with.

Incidents in the security world usually imply that an external (although sometimes internal) hostile party has unauthorized access to, or control of, systems that support your organization's core processes. Many organizations can be compromised for a great deal of time before it is discovered. As a general rule, most organizations declare something an *incident* at the point at which security analysts from the outside must be brought in to remediate a situation.

What Defines a Breach?

In legal terms, breaches represent a significant loss of data to an unauthorized external party, and may require public disclosure of the loss according to law. A network may be attacked many thousands of times without worry, be compromised (and recover from it) many times during the year, but still continue doing business uninterrupted, as long as it is not breached.

What to Include in Your Incident Remediation Plan

One of the great benefits of security monitoring is not only detecting when security controls have failed, but *how* they failed, and then rolling that information back into improving overall security.

When a host is compromised by means of a malicious website, cleaning the infected host is only part of the response. On the other hand, blocking the malicious website to prevent any further infections proves the real worth of security monitoring.

Security monitoring without this kind of root cause analysis treats only the symptoms, not the disease. For this reason, make sure that when planning the deliverables from your incident response plan, that you not only emphasize fixing compromised systems, but also collecting information to remediate the problems that caused the compromise to prevent them from occurring again.

Developing an Effective Triage Strategy

The term *triage* is more commonly used within the medical community, where it means saving lives by helping emergency medical personnel rapidly assess wound or illness severity, and establish the right protocols, in the right order to reduce trauma and sustain patient health and recovery. However, these same principles can be applied to security analysis as well. Some guidelines to help you perfect your ability to triage information security incident types might include the following:

- How to identify the various types of security incidents, by understanding how attacks unfold.
- How to prioritize remediation efforts, for example, to identify which incidents to investigate first by what potential threats could cause the most damage to your business.
- How to effectively respond in crisis situations.

These are just a few ideas to consider in defining triage efforts within your incident response planning. You will likely want to consider more triage and incident response practices based on your specific environment, and your specific compliance and network security requirements.

How Do I Discover a Possibly Larger Attack in Progress?

Most day-to-day security monitoring work involves detecting where security controls have failed and a system has become compromised by malware or exploits. However, situations will always exist that require more investigation, with reason to believe that one compromised host may have been used to compromise others, or a more complex sequence of specific events can be used to carry out an attack or exploit, commonly referred to as an *attack vector*.

Indicators of Compromise (IoCs)

Indicators of compromise, or IoCs, represent pieces of information about an attack vector. An IoC can be used to observe a relationship to other attacks. In fact, if you see an IoC responsible for multiple malware infections that all take instructions from the same remote

host on the internet, you should track it. This allows you to disable many infections at the same time by blocking that server

For related information about IoCs comprising Open Threat Exchange®(OTX) *pulses*, see [What is Open Threat Exchange®?](#)

Common Attack Vectors and Strategies to Combat Them

The best way to determine the appropriate incident response in any given situation is to understand what types of attacks your organization may most logically face.

The National Institute of Standards and Technology (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>) publishes the following list of common attack vectors:

- **External/Removable Media**

An attack executed from removable media (for example, flash drive, CD) or a peripheral device.

- **Attrition**

An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.

- **Web**

An attack executed from a website or a web-based application (for example, drive-by download).

- **Email**

An attack executed via an email message or attachment (for example, malware infection).

- **Improper Usage**

Any incident resulting from violation by an authorized user of the acceptable usage policies established by an organization, excluding the above categories.

- **Loss or Theft of Equipment**

The loss or theft of a computing device or media used by the organization, such as a laptop or smart phone. Identify which pieces of equipment would cause the greatest risk to the company in the event of loss or theft. In most companies, the laptop belonging to the CFO would be included along with any server hard drive containing IP or other sensitive

data.

- **Other**

An attack that does not fit into any of the other categories.

Review the foregoing list to make sure that you have security policies and controls in place to mitigate the majority of risks from these attack vectors. Also, use this list to guide your team in determining how to classify the various types of security incidents.

Alert Taxonomy

An alert taxonomy can help you to order related alerts into a picture of a larger attack in progress, as the attacker does the following:

- Performs reconnaissance.
- Delivers the attack to many systems.
- Successfully exploits some of them.
- Uses the compromised system as a base from which to attack others.

Get Inside the Mind of the Attacker Through Security Event Categorization

Traditional information security falsely assumes that you know which path an attacker will take through your network. For example, attackers rarely come through your front door, or in this context, your gateway firewall. On the other hand, each attack *does* generally follow a certain pattern, or what Lockheed Martin calls the Cyber Kill Chain®.

The Cyber Kill Chain is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it. Each stage demonstrates a specific goal along the attacker's path. Designing your monitoring and response plan around the cyber kill chain model is an effective method, because it focuses on how actual attacks happen.

Cyber Kill Chain model

Intent	Attacker Goal
Reconnaissance & Probing	<ul style="list-style-type: none"> • Find target. • Develop plan of attack based on opportunities for exploitation.
Delivery & Attack	<ul style="list-style-type: none"> • Place delivery mechanism on line. • Use social engineering to get target to access malware or other exploit.

Cyber Kill Chain model (Continued)

Intent	Attacker Goal
Exploitation & Installation	<ul style="list-style-type: none"> • Exploit vulnerabilities on target systems to acquire access. • Elevate user privileges and install persistence payload.
System Compromise	<ul style="list-style-type: none"> • Exfiltrate high-value data as quietly and quickly as possible. • Use compromised system to gain additional access, "steal" computing resources, and/or use in an attack against someone else.

When devising an incident response plan, you may find it helpful to prioritize security events or alarms.

Sample incident response spreadsheet

Incident Type	Kill Chain Stage	Priority Level	Recommended Action
Port scanning	Reconnaissance & probing	Low	You can ignore these unless AlienVault OTX IP Reputation gives the IP responsible a bad score. OTX IP Reputation stores reports on any suspicious IP activity, which may or may not be malicious. See What is Open Threat Exchange®? .
Malware infection	Delivery & attack	Low-Medium	Remediate malware infections as quickly as possible before they progress. Scan the rest of your system for related IoCs, for example, MD5 hashes. See What is Open Threat Exchange®? .
Distributed denial of service	Exploitation & Installation	High	Configure web servers to protect against HTTP and SYN flood requests. Coordinate with your Internet service provider (ISP) during an attack to block the responsible IPs.
Unauthorized access	Exploitation & Installation	Medium	Detect, monitor, and investigate unauthorized access attempts—with priority on those that are mission-critical and/or contain sensitive data.

Sample incident response spreadsheet (Continued)

Incident Type	Kill Chain Stage	Priority Level	Recommended Action
Insider breach	System compromise	High	<p>Identify the privileged user accounts for all domains, servers, applications, and critical devices.</p> <p>Make sure that you enabled monitoring for all systems, and for all system events.</p> <p>Verify that your USM Appliance raw log infrastructure is actively recording all events.</p>
Unauthorized privilege escalation	Exploitation & installation	High	<p>Through its built-in correlation directives, USM Appliance automatically records all privileged escalation events, and sends alarms for unauthorized attempts.</p> <p>Depending on requirements, you may also enhance your USM Appliance environment by adding custom correlation directives.</p>
Destructive attack on systems, data.	System compromise	High	<p>Back up all critical data and systems; test, document, and update system recovery procedures.</p> <p>During a system compromise, capture evidence carefully. Document all recovery steps and all evidential data.</p>
Advanced persistent threat (APT) or multistage attack	Represents all stages from reconnaissance through system compromise	High	<p>Any of the individual events illustrated could represent part of an APT, the most formidable type of security threat. For that reason, view each event as part of a larger context, incorporating the latest threat intelligence.</p> <p>USM Appliance correlation directives often look at how many events of a specific nature occurred before generating an alarm, thereby increasing its reliability. OTX pulses, on the other hand, require only one event to do so.</p>

Sample incident response spreadsheet (Continued)

Incident Type	Kill Chain Stage	Priority Level	Recommended Action
False alarms	Represents all stages.	Low	Much of the job of an incident responder consists of eliminating irrelevant information and removing false positives. This process is continuous. For more information, see Establishing Baseline Network Behavior and also Use of Policies in USM Appliance .
Other	All stages	High	Incident response never stops and provides a source for continuous improvement. Over time, as you see events turn into alarms, you gather knowledge that helps you discover new ways to categorize events and to prevent them from becoming alarms in the first place.

About Port Scanning Alarms

You may feel certain that attackers are getting no useful information from their scanning. However, if their scans of your external systems appear to be detailed and comprehensive, you can reasonably assume that they have the intent to follow up the reconnaissance with attack attempts later on.

If the scanning originates from a legitimate organization's networks, your best approach is to contact their security team, if they have one, or network management personnel.

If no contact details are apparent, look for details about the domain in WHOIS, a link to which is available at the bottom of the USM Appliance Security Events list and also from the applicable OTX web pages for such IoCs.



Note: Blocking the source address may be counter productive, and merely cause the attacker to use a different source address.

¹This topic is adapted from Jaime Blasco, "Building an Effective Incident Response Framework Infographic" The AlienVault Blogs 2014 <https://cybersecurity.att.com/blogs/security-essentials/incident-response-framework-infographic>; Lauren Barraco, "Defend Like an Attacker: Applying the cyber kill chain." The AlienVault Blogs 2014. <https://cybersecurity.att.com/blogs/security-essentials/defend-like-an-attacker-applying-the-cyber-kill-chain>; and "The Insider's Guide to Incident Response eBook" AlienVault Resource Center. 2015. <https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response-download>.

USM Appliance Reports

This section covers the following subtopics:

- About USM Appliance Reports376
- How to Run Reports377
- Create Custom Reports382
- Create Custom Reports from SIEM Events or Raw Logs385
- List of USM Appliance Reports387

About USM Appliance Reports

AlienVault USM Appliance includes hundreds of predefined reports to keep you informed about assets, level of compliance, alarms, and security events in your organization. Starting from USM Appliance version 5.2, AlienVault delivers new reports in threat intelligence updates instead of platform updates, allowing for more frequent updates and improvements on USM Appliance reports. See [List of USM Appliance Reports](#) for a complete list of reports.

Report Categories

USM Appliance groups reports into different categories for easy access. The following table summarizes the categories.

USM Appliance report categories

Report Categories	Description
Alarms	Reports on top alarms, top attackers, top attacked hosts, and top destination ports.
Assets	Reports on assets, including asset properties, vulnerabilities, events, alarms, and raw logs for selected assets.
Compliance	Reports on various compliance regulations, including FISMA, HIPAA, ISO 27001, PCI 2.0, PCI 3.0, PCI DSS 3.1, and SOX. These reports display information such as events, alarms, and asset, and map them to compliance requirements.
Raw Logs	Reports on raw logs from different sources, such as firewalls, IDS/IPS systems, mail security devices, and antivirus applications.
Security Events	Reports on security events from different sources, such as events coming from firewalls, IDS/IPS systems, mail security devices, and anti-virus applications. In USM Appliance version 5.2, reports on OTX pulses and OTXIP reputation are also included.
Security Operations	Reports on security operations including tickets, top alarms, and top security events.
Tickets	Reports on tickets opened on events, alarms, metric, vulnerabilities, and anomalies.
User Activity	Report on user activity in the USM Appliance web interface.
Custom Reports	User customized reports including cloned reports and the custom security events or custom raw logs reports.

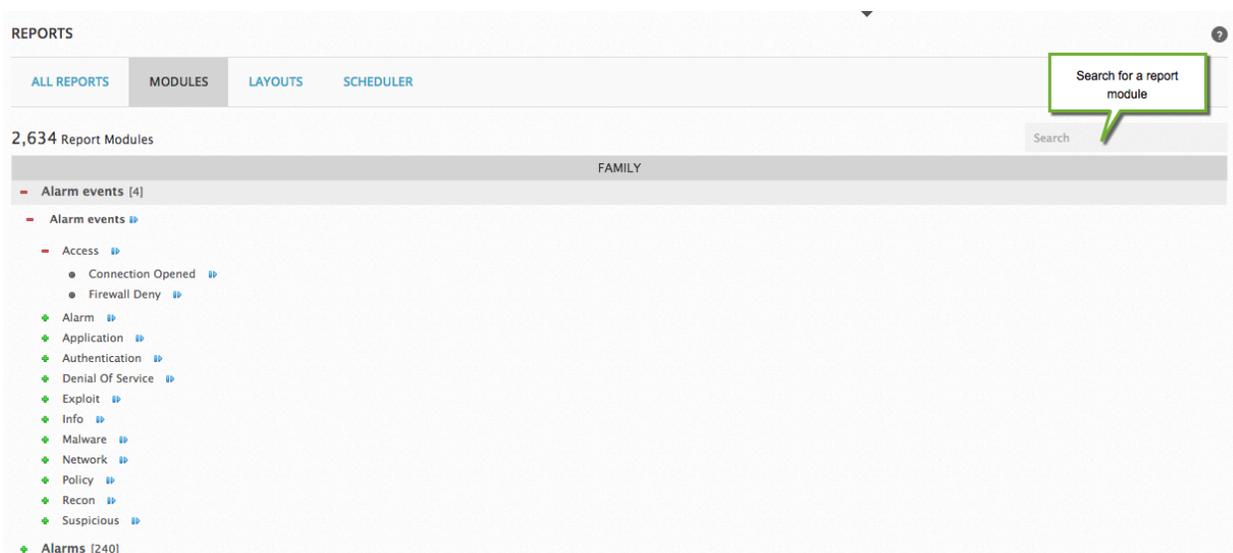
Report Modules

The USM Appliance reports consist of two basic components:

- A module defines queries to the database or file system, in order to retrieve the data necessary for table and graph generation.
- A layout defines the graphical aspects of a report, such as logo, header and footer, and color scheme.

You can generate reports based on a combination of several modules and a single layout. By default, USM Appliance contains more than 2,600 modules and one basic layout.

The USM Appliance organizes the report modules into categories. Go to **Reports > All Reports > Modules** and expand the categories by clicking the green plus sign (+) next to the category name. You can further extend each subcategory, eventually reaching an individual event category in the module.



How to Run Reports

You can find all the USM Appliance reports on **Reports > All Reports**.

Report fields and descriptions

Fields		Descriptions
Report		Name of the report.
Category		Category that the report belongs to.
Settings		Default settings to run the report—on all assets, for the last 30 days, and with the default layout.
Scheduled		Whether the report is scheduled to run in the future or not.
Actions		To delete the report. Not available for built-in reports.
		To export the report.
		To copy the report.
		To edit the report. Not available for built-in reports.
		To customize the parameters before running.
		To run the report without any modification.

This section covers the following subtopics:

- Run the Reports
- Schedule a Report to Run Regularly
- Export a Report

Run the Reports

To see the modules that the report includes

- Click the report row.

A list of modules displays below.

The screenshot shows the 'REPORTS' section of the interface. It includes tabs for 'ALARM REPORTS', 'MODULES', 'LAYOUTS', and 'SCHEDULER'. A search bar is present, and a list of reports is displayed. The 'Alarm Report' is selected, and its details are shown in a modal window. The 'Report includes' section lists the following modules:

- Title Page [Main Title = Alarm Report, Date = #DATE]
- Alarms - Top Attacked Host [Top Attacked Host = 10]
- Alarms - Top Attacker Host [Top Attacker Host = 10]
- Alarms - Top Destination Ports [Top Destination Ports = 10]
- Alarms - Top Alarms [Top Alarms = 15]
- Alarms - Top Alarms by Risk [Top Alarms by Risk = 15]

The report settings are: Assets: All Assets, Date Range: Last 30 days, Layout: Default, and it is not scheduled.

To run a report without any modification

1. Select a report.
2. (Optional) Examine the modules that the report includes.
3. Click the Run icon (▶).

The report runs on all assets and for the last 30 days. The result displays after the completion.

To change the date range, the layout, and/or the assets covered in the report

1. Select a report.
2. (Optional) Examine the modules that the report includes.
3. Click the Custom Run icon (⊞).

- In Custom Run, perform one or all of the following:
 - Change the date range.

Note: In USM Appliance version 5.2 or earlier, the **Last x days** options exclude the current day. In USM Appliance version 5.2.1 or later, these options include the current day.

- Select a different layout. For instructions, see [Create Custom Report Layouts](#).
 - Specify an asset or a group of assets.
- Click **Run**.

The generated report displays after completion.

- (Optional) To save or distribute the report, click **Export**.

You can choose **PDF** or **XLSX** format, either download the file locally or send it through email.

If choosing **Email**, type the email address in the box that appears, use semicolon to separate multiple addresses.

- Click **Export**.

Note: In order to send reports by email, you need to have configured the mail relay settings in USM Appliance. For instructions, see "Configuring Mail Relay in USM Appliance" in the Initial Setup section of the *USM Appliance Deployment Guide*.

Schedule a Report to Run Regularly

Depending on the type of report, the date range, and the number of assets to include, generating a report may take a while. In this case, you can schedule a report to run during off-peak hours, when the system has lower utilization. You can also set the report to run regularly based on your needs.

To schedule a report

1. Go to **Reports > All Reports**, and then click **Scheduler**.
2. Click **Schedule a Report**.
3. In **Select Report**, click the **+** sign next to the report name or drag the report to the left column. Alternatively, type the name of the report in the search box to find a specific report.



Note: You can only select one report per scheduler.

4. In **File Type**, select PDF or XLSX.
5. (Optional) In **E-mails**, enter a list of email addresses, separated by semicolons, for people to receive the report.
6. In **Date**, select the date range for the report.
7. (Optional) Select a user or entity that can access the report.
8. (Optional) If you only want to store the last generated report, disable **Save in Repository**. Otherwise USM Appliance stores all reports generated by the scheduler.
9. Select the frequency as well as the date and time that you want the report to run.
10. (Optional) Select the assets that you want to include in the report.
11. Click **Save Scheduler**.

USM Appliance creates the scheduler and generates the report based on the schedule you have configured.

To download the reports

1. Go to **Reports > All Reports > Scheduler**.
2. Click the disk icon () for the scheduled report.
3. In **View PDF Repository**, click the PDF icon next to the report.

Export a Report

In order to save your work and time, you can export a report, especially a custom report to a different USM Appliance system, and use it there.

To export a report in the USM Appliance

1. Select the report you want to export.
2. (Optional) Examine the modules that the report includes.
3. Click the download icon ()
4. Enter a password to encrypt the report, and then click **OK**.



Note: You will need to enter this password while importing the report.

Your browser downloads the report to your local system or prompts you for the download.

To import the report on another USM Appliance

1. Login to the USM Appliance web interface and go to **Reports > All Reports**.
2. From the **Actions** list at the upper right-hand corner, select **Import Report**.
3. In Import Report, click **Choose File** to select the report you want to import.
4. Enter the password used to encrypt the report, click **Import**.

The report appears as a custom report under **Reports > Custom Reports**.



AlienVault OSSIM Limitations: In the AlienVault OSSIM environment, users are limited in their reporting abilities.

Create Custom Reports

If predefined reports in USM Appliance do not suit your needs, you can either modify an existing report or generate a new report from scratch. Both options use the Report Wizard.



Note: In order to add the custom report as a dashboard widget, keep the report name under 42 characters.

This section covers the following subtopics:

- [Modify Built-in Reports](#)
- [Create a New Report from Scratch](#)
- [Create Custom Report Layouts](#)

Modify Built-in Reports

So that you can continue to receive improvements to your built-in USM Appliance reports from USM Appliance updates, if you want to modify a report, you need to modify a copy of the report.

To modify a built-in report

1. Select a report you want to modify.
2. Click the copy icon ()
3. By default, the system adds "_1" to the original name of the report. Modify it if you want, and then click **Save**.

The Report Wizard displays.

4. Go through the wizard to make modifications as needed.
 - In step 1, you can add modules to or remove them from the report.
 - In step 2, you can change the asset selection.
 - In step 3, you can modify the parameters for the selected report modules. For example, you can set DS Group to cut down the number of events covered in the report.



Note: You cannot change the graphs or tables.

5. To save the report without running it, click **Save**; to save the report and run it immediately, click **Save & Run**.

The report appears in Custom Reports. You can run it the same way as a USM Appliance built-in report, and you can modify the settings in the report by clicking the edit icon () , which will run through the Report Wizard again.

Create a New Report from Scratch

You can create a new custom report from scratch by going through the Report Wizard.

To create a new custom report

1. Go to **Reports > All Reports**, and then in **Actions** select **Create Report**.

The Report Wizard displays.

1. Go through the wizard as follows,
 - In step 1, type a name for the report, modify the date range, and then select the modules you want to use.
 - In step 2, select the asset(s) you want to include.
 - In step 3, modify the parameters for the selected report modules, as needed. For example, you can set the DS Group to cut down the number of events covered in the report.
2. To save the report without running it, click **Save**; to save the report and run it immediately, click **Save & Run**.

The report appears in Custom Reports. You can run it the same way as a USM Appliance built-in report, and you can modify the settings in the report by clicking the edit icon () , which will run through the Report Wizard again. By default, a custom report does not include a title page. If you want to include a title page, add the **Title Page** module in step 1 of the wizard.



Important: If the user who created a scheduled report is deleted from USM Appliance, the scheduled reports they had created will also be removed.

Create Custom Report Layouts

If the default look and feel of reports does not suit your company's requirements, you can create a custom layout with customized icons, footers, and/or color schemes.

To create a custom layout

1. Go to **Reports > All Reports**, and then **Layouts**.
2. Click **New Layout**.
3. In the **Name** field, type a name for the new layout.
4. In the **Permissions** field, select All or the context that has permission to use this layout.
5. Select the background and foreground colors for the title and subtitles.
6. Customize the left and right footers. The parameters display on the right-hand side.

USM Appliance replaces the parameters in the footer with actual values when running the report.

7. Upload an image file (.gif, .png, or .jpg) to use in the header for the PDF report.
8. Click **Save**.

You can use the layout when modifying a report or creating a new report.

Create Custom Reports from SIEM Events or Raw Logs

If the available report modules do not suit your needs, you can generate your own module, which defines the data that will be included in a report.

This section covers the following subtopics:

- [Create Custom Reports from Security Events](#)
- [Create Custom Reports from Raw Logs](#)
- [Save a Customized Module as a New Report Module](#)

Create Custom Reports from Security Events

Occasionally you may want to generate a report from the security events that USM Appliance detects in your environment. To do that, you need to create a report module first.

To create a custom report from security events

1. Go to **Analysis > Security Events (SIEM)** and perform a search to include the events you want to see.
2. Click **Change View** to select a predefined view.

Predefined views include Default, Taxonomy, Reputation, Detail, Risk Analysis, and IDM. Each view displays the same events but with different columns.

3. Alternatively, click **Change View** and then select **Create New View**.
 - a. In Create New Custom View, select the columns you want to see in this view.
 - b. To apply the same query every time when you launch this view, select **Include custom search criteria in this predefined view**.
 - c. Type a name for the view, and then click **Create**.

USM Appliance saves your changes and refreshes the page to display the view.

4. Click **Change View** again and select **Edit Current View**.

- In Edit Current View, click **Save as Report Module** at the bottom.
- Go to **Reports > All Reports**, click **Modules**, and then expand **Custom Security Events**.

See the new module listed. It has the same name as the custom view.

- To generate the report, click the blue arrow next to the module's name, and then go through the Report Wizard.

Notice that the report module, Custom Security Events - <name of your custom view>, is already selected for you.

- Alternatively, follow the steps in [Create a New Report from Scratch](#) and add the new report module yourself.

USM Appliance saves the custom report under **Reports > All Reports > Custom Reports**. You can then run the custom reports as other built-in reports.

Create Custom Reports from Raw Logs

In addition to creating a report module from security events, you can also create one from raw logs.

To create a custom module from raw logs

- Go to **Analysis > Raw Logs** and perform a search to include the entries you want to use in the report.
- Click **Predefined Searches**. In the text box type a name for the search, and then click **Add**.

3. Go to **Reports > All Reports**, click **Modules**, and then expand **Raw Logs**.



Note: USM Appliance saves the raw log search in a report module called **Custom List**, but you cannot choose it until you run the Report Wizard.

4. Click the blue arrow next to **Custom List**, and then go through the Report Wizard.
Notice that the report module, Raw Logs - Custom List, is already selected for you.
5. Alternatively, follow the steps in [Create a New Report from Scratch](#) and add the new report module yourself.
6. In Step 3 of the wizard, from **Filter**, select the query you saved before running the report.

USM Appliance saves the custom report under **Reports > All Reports > Custom Reports**. You can then run the custom reports as other built-in reports.

Save a Customized Module as a New Report Module

In the USM Appliance built-in reports, each report module only appears once. Sometimes you may want to use the same module multiple times, but with different parameters. For example, you may want to generate a report on all alarms ordered by different DS groups. In this scenario, you need to save the corresponding report module as a new report module, and then add it while building the custom report.

To create a new module from an existing one

1. Run a report following the instructions in [Modify Built-in Reports](#).
2. In Step 3 of the wizard, locate the module you want to duplicate, change the parameters of the module as desired, and then click **Add as a New Report Module**.
3. In **Add a New Subreport**, type a name and click **Add**.

USM Appliance saves the module with the changed parameters.

To use the new module in a report

1. Create a new report. For instructions, see [Create Custom Reports](#).
2. In Step 1 of the wizard, search for the module you just saved, and then add it to your report.
3. Add more modules if you want and finish running the wizard.

List of USM Appliance Reports

AlienVault updates the USM Appliance reports on an on-going basis. The following table lists the reports in alphabetical order according to their category.

List of Reports

Category	Report Title
Alarms	Alarm Report
	Malware Alarms
Asset	Asset Compliance Report
	Asset Report
	Availability Report
Compliance	Vulnerabilities Report
	Application Exploits
	Business and Compliance
	DFARS Default Account Usage
	DFARS Remote Access Report
	DFARS Unencrypted Traffic
	FERPA Default Account Usage
	FERPA Remote Access Report
	FERPA Unencrypted Traffic
	FISMA Report
	GLBA: File Adds or Deletes
	GLBA: File Changes
	GLBA: Firewall User Changes
GLBA: Group Changes	
GLBA: MAC Address Changes	
GLBA: Policy and Configuration Changes	
GLBA: Registry Changes	
GLBA: System Failed Logins	

List of Reports (Continued)

Category	Report Title
	GLBA: System Successful Logons
	GLBA: System Time Changes
	GLBA: User Account Changes
	GLBA: User Activity
	HIPAA Report
	HIPAA: Account Lockouts
	HIPAA: Account Unlock Report
	HIPAA: Authentication Failed Logins
	HIPAA: Database Failed Logons
	HIPAA: Database Successful Logons
	HIPAA: Failed Logins
	HIPAA: Failed Logon to Firewall
	HIPAA: FTP Failed Logons
	HIPAA: FTP Successful Logons
	HIPAA: List of identified ePHI assets
	HIPAA: List of identified ePHI assets with Services
	HIPAA: Password Change Status
	HIPAA: Successful Logon to Firewall
	HIPAA: System Failed Logins
	HIPAA: System Successful Logons
	ISO 27002: Accounts Locked Out
	ISO 27002: Accounts Unlocked
	ISO 27002: Active Directory Group Additions
	ISO 27002: Active Directory Group Removals

List of Reports (Continued)

Category	Report Title
	ISO 27002: Administrative Logon
	ISO 27002: Antivirus Disabled
	ISO 27002: Antivirus Events Detected
	ISO 27002: Assets with Vulnerabilities
	ISO 27002: Database Failed Logons
	ISO 27002: Database Successful Logons
	ISO 27002: Failed Logon to Firewall
	ISO 27002: FTP Failed Logons
	ISO 27002: FTP Successful Logons
	ISO 27002: Identified Services on a Group of Systems
	ISO 27002: List of Identified Assets
	ISO 27002: Successful Logon to Firewall
	ISO 27002: System Failed Logons
	ISO 27002: System Successful Logons
	NERC CIP: IPv6 Detection
	NERC CIPv5: Antivirus Details
	NERC CIPv5: Antivirus Disabled
	NERC CIPv5: Current Vulnerabilities Report
	NERC CIPv5: Database Failed Logons
	NERC CIPv5: Database Successful Logons
	NERC CIPv5: Failed Logon to Firewall
	NERC CIPv5: File Adds or Deletes
	NERC CIPv5: File Changes
	NERC CIPv5: FTP Failed Logons

List of Reports (Continued)

Category	Report Title
	NERC CIPv5: FTP Successful Logons
	NERC CIPv5: List of identified BES Cyber Assets
	NERC CIPv5: List of identified BES Cyber Assets with Services
	NERC CIPv5: MAC Address Changes
	NERC CIPv5: New Software Installed
	NERC CIPv5: Password Change Status
	NERC CIPv5: Registry Adds or Deletes
	NERC CIPv5: Registry Changes
	NERC CIPv5: System Failed Logins
	NERC CIPv5: System Successful Logons
	NERC CIPv5: USM Appliance User Activity
	NIST 800-171 Default Account Usage
	NIST 800-171 Remote Access Report
	NIST 800-171 Unencrypted Traffic
	PCI 2.0 Report
	PCI 3.0 Report
	PCI DSS 3.2: All Antivirus Security Risk Events
	PCI DSS 3.2: All Virus Events
	PCI DSS 3.2: Encrypted Networks Having Unencrypted APs
	PCI DSS 3.2: Access Control Device Denied
	PCI DSS 3.2: Account Lockouts
	PCI DSS 3.2: Account Unlock Report
	PCI DSS 3.2: Admin Access to Systems
	PCI DSS 3.2: Antivirus Definition Updates

List of Reports (Continued)

Category	Report Title
	PCI DSS 3.2: Antivirus Disabled
	PCI DSS 3.2: Antivirus Failed Updates
	PCI DSS 3.2: Authentications with Default Credentials
	PCI DSS 3.2: Cloaked Wireless Networks with Uncloaked APs
	PCI DSS 3.2: Database Configuration Changes
	PCI DSS 3.2: Database Errors
	PCI DSS 3.2: Database Failed Logins
	PCI DSS 3.2: Database Successful Logins
	PCI DSS 3.2: Database Users Added
	PCI DSS 3.2: Database Users Removed
	PCI DSS 3.2: Dropped or Denied Connections
	PCI DSS 3.2: Encrypted HTTPS Connections
	PCI DSS 3.2: Encrypted VPN Client Connections Accepted
	PCI DSS 3.2: Encrypted VPN Client Connections Failed
	PCI DSS 3.2: Environment User Activity
	PCI DSS 3.2: Failed Logins
	PCI DSS 3.2: Firewall Configuration Changes
	PCI DSS 3.2: Firewall Failed Authentication
	PCI DSS 3.2: Firewall Intrusion Detection
	PCI DSS 3.2: Firewall Successful Authentication
	PCI DSS 3.2: Firewall User Changes
	PCI DSS 3.2: Group Changes
	PCI DSS 3.2: Infected Computers
	PCI DSS 3.2: Information Security Policy Compliance Checks

List of Reports (Continued)

Category	Report Title
	PCI DSS 3.2: Information Security Policy Compliance Failed
	PCI DSS 3.2: Intrusion Detection Events
	PCI DSS 3.2: Security Device Policy Modifications
	PCI DSS 3.2: Successful Logins
	PCI DSS 3.2: Suspicious Clients on Wireless Networks
	PCI DSS 3.2: Suspicious Database Events
	PCI DSS 3.2: System Time Changes
	PCI DSS 3.2: User Management Activity
	PCI DSS 3.2: Vulnerability Details
	PCI DSS 3.2: Wireless Networks
	PCI DSS 3.2: Wireless Networks Using Weak Encryption
	PCI: File Integrity Changes
	PCI: User Management Activity
	SOX Report
Raw Logs	Raw Logs
	Raw Logs: Access
	Raw Logs: Alarm
	Raw Logs: Alert
	Raw Logs: Anomaly Detection
	Raw Logs: Antivirus
	Raw Logs: Application
	Raw Logs: Application Firewall
	Raw Logs: Applications
	Raw Logs: Authentication

List of Reports (Continued)

Category	Report Title
	Raw Logs: Authentication and DHCP
	Raw Logs: Availability
	Raw Logs: Data Protection
	Raw Logs: Database
	Raw Logs: Denial of Service
	Raw Logs: Exploit
	Raw Logs: Firewall
	Raw Logs: Honeypot
	Raw Logs: Info
	Raw Logs: Infrastructure Monitoring
	Raw Logs: Intrusion Detection
	Raw Logs: Intrusion Prevention
	Raw Logs: Inventory
	Raw Logs: Mail Security
	Raw Logs: Mail Server
	Raw Logs: Malware
	Raw Logs: Management Platform
	Raw Logs: Network
	Raw Logs: Network Discovery
	Raw Logs: Operating System
	Raw Logs: Other Devices
	Raw Logs: Policy
	Raw Logs: Proxy
	Raw Logs: Reconnaissance

List of Reports (Continued)

Category	Report Title
	Raw Logs: Router/Switch
	Raw Logs: Server
	Raw Logs: Suspicious
	Raw Logs: System
	Raw Logs: Unified threat management
	Raw Logs: Voip
	Raw Logs: VPN
	Raw Logs: Vulnerability Scanner
	Raw Logs: Web Server
	Raw Logs: Wireless
	Raw Logs: Wireless Security/Management
Security Events	Activity from OTX Pulses
	Activity with OTX IP Reputation Information
	Database Activity
	Events by Data Source
	Events by Product Type
	Events by Source Category
	Geographic Report
	Security Events: Access
	Security Events: Account Changes
	Security Events: Admin Access
	Security Events: Alarm
	Security Events: Alert
	Security Events: Anomaly Detection

List of Reports (Continued)

Category	Report Title
	Security Events: Antivirus
	Security Events: Application
	Security Events: Application Firewall
	Security Events: Applications
	Security Events: Authentication
	Security Events: Authentication and DHCP
	Security Events: Availability
	Security Events: Data Protection
	Security Events: Database
	Security Events: Denial of Service
	Security Events: Exploit
	Security Events: Firewall
	Security Events: Honeypot
	Security Events: Impacts
	Security Events: Info
	Security Events: Infrastructure Monitoring
	Security Events: Intrusion Detection
	Security Events: Intrusion Prevention
	Security Events: Inventory
	Security Events: Mail Security
	Security Events: Mail Server
	Security Events: Malware
	Security Events: Management Platform
	Security Events: Network

List of Reports (Continued)

Category	Report Title
	Security Events: Network Discovery
	Security Events: Operating System
	Security Events: Other Devices
	Security Events: Policy
	Security Events: Proxy
	Security Events: Reconnaissance
	Security Events: Report
	Security Events: Router/Switch
	Security Events: Server
	Security Events: Suspicious
	Security Events: System
	Security Events: Unified threat management
	Security Events: User Activity
	Security Events: VoIP
	Security Events: VPN
	Security Events: Vulnerability Scanner
	Security Events: Web Server
	Security Events: Wireless
	Security Events: Wireless Security/Management
	Unique Signatures by Data Source
	Unique Signatures by Product Type
	Unique Signatures by Source Category
	Honeypot Activity
	Policy and Configuration Changes

List of Reports (Continued)

Category	Report Title
	Security Operations Report
Tickets	Ticket Report
	Ticket Status
User Activity	User Activity

User Administration

This section covers the following subtopics:

- User Administration in USM Appliance 400
- USM Appliance User Accounts 401
- User Authentication 402
- User Authorization 408
- Manage User Accounts 418
- Monitor User Activities 428

User Administration in USM Appliance

In AlienVault USM Appliance, user administration occurs through authentication and authorization, which includes the process of creating, modifying, or deleting user accounts; controlling access to the USM Appliance web interface; enforcing administrative policies; and monitoring user activity.

User Authentication

USM Appliance allows you the flexibility of verifying user authenticity by storing credentials locally in USM Appliance or with existing user credentials established with LDAP (Lightweight Directory Access Protocol).

See [Set Up Password Policy for Local User Authentication](#) for instructions to store user credentials locally, or [Configure LDAP in USM Appliance](#) for instructions to use LDAP for authenticating users.

User Authorization and RBAC

Role-based access control (RBAC) delegates certain functions to specific roles and can be instrumental in enforcing administrative policies. The role, a given set of responsibilities, determines which USM Appliance features users can access. You may want to restrict access to certain parts of the web interface to ensure that unauthorized changes aren't made to USM Appliance. For example, you can restrict access solely to the part of the UI for delegating and reporting tickets, while allowing broader access to more critical parts of the UI for defining policies and correlation directives.



Important: You must configure user permissions in USM Appliance, even if authentication is performed against LDAP.

See [User Authorization](#) for more details.

User Activity

In addition to authenticating and authorizing users, USM Appliance captures the length of user sessions, as well as their activities. You can use these data for system audits and compliance.

See [Monitor User Activities](#) to make logging selections for monitoring user activity.

User Accounts

When you create user accounts, you determine what role the user is going to play in viewing and administering USM Appliance. You configure which parts of the web interface the users have access to and their level of visibility into the company's assets, including USM Appliance Sensors.

See [Manage User Accounts](#) for topics and instructions for creating and managing user accounts.

USM Appliance User Accounts

USM Appliance has different levels of user accounts for administration and management:

- **Root user** — Created during the USM Appliance installation. The root user is equivalent to a Linux root user. The root user and the default admin may be the same person in the organization.

The root user

- Can access and perform all operations in the USM Appliance console (the command line interface).
- Can reset password for all users including the default admin user.

- **Default admin** — Created the first time a user accesses the USM Appliance web UI. A default admin is typically responsible for ensuring the security of the company network.

The default admin is created when you first install USM Appliance. By default, USM Appliance gives this user the username *admin*, which cannot be changed. If you want to review the instructions for creating the default admin user, see "Create the Default Admin User" in the Initial Setup section of the *USM Appliance Deployment Guide*.

The default admin

- Has complete access and visibility into the USM Appliance web UI.
- Has full administrative privileges.
- Can create admins with full access to the USM Appliance web UI and users with varying degrees of access to specific USM Appliance components.
- Can reset password for self, admin, and normal users.

- **Admin** — Created by the default admin to help administer USM Appliance. Admins may be members of the IT department who are responsible for assisting with network infrastructure. The default admin determines the level of access for each admin.

An admin

- Has all the administrative privileges of the default admin.
 - Cannot delete the default admin.
 - Can reset password for self, other admin, and normal users.
- **Users** — Created by an admin and have varying degrees of access to the USM Appliance web UI. Users may be responsible for tasks such as generating reports or administering tickets.

A user

- Can view the parts of USM Appliance that have been granted to them by an admin.
- Can see only the activity of other users who belong to the same entity as they do.
- Can update their own account including password reset.
- Cannot create other user accounts.

User Authentication

USM Appliance allows you the flexibility of verifying user authenticity by storing credentials locally in USM Appliance or with existing user credentials established with LDAP (Lightweight Directory Access Protocol).

See [Set Up Password Policy for Local User Authentication](#) for instructions to store user credentials locally, or [Configure LDAP in USM Appliance](#) for instructions to use LDAP for authenticating users.

Set Up Password Policy for Local User Authentication

If you decide to use authentication occurring locally in USM Appliance, AlienVault encourages you to set up the password policy according to your company's security standard. All web user passwords are encrypted by applying the SHA-256 algorithm with a [salt](#), and then stored in the database. You can also configure the account lockout period when setting up the policy.



Note: AlienVault stores the USM Appliance root user password directly on the system, after applying SHA-512 with a salt. By default, only the root user account can access the USM Appliance CLI. You cannot configure a lockout period for the root user.

For assistance with creating new users in USM Appliance, see [Create New Accounts for Local Users](#).

To configure password policy for USM Appliance

1. In the USM Appliance web interface, go to **Configuration > Administration > Main** and expand the **Password Policy** section.

ADMINISTRATION

USERS MAIN BACKUPS

BACKUP

IDM

TICKETS

LOGIN METHODS/OPTIONS

METRICS

OPEN THREAT EXCHANGE

USM FRAMEWORK

PASSWORD POLICY

Find Word SEARCH

ENABLE DESKTOP NOTIFICATIONS

UPDATE CONFIGURATION

Save changes

Password policy

Setup login password policy options

Minimum password length	<input type="text" value="7"/>	?
Maximum password length	<input type="text" value="32"/>	?
Password history	<input type="text" value="0"/>	?
Complexity	<input type="text" value="No"/>	?
Minimum password lifetime in minutes	<input type="text" value="0"/>	?
Maximum password lifetime in days	<input type="text" value="0"/>	?
Failed logon attempts	<input type="text" value="5"/>	?
Account lockout duration	<input type="text" value="5"/>	?

2. Type the values for password authentication that are required by your company or organization, as illustrated by the [Password Policy Configurations](#) table.
3. Click **Update Configuration**.

Password Policy Configurations

Parameter	Description	Default Setting
Minimum password length	Minimum number of characters for a password.	7
Maximum password length	Maximum number of characters for a password.	32
Password history	Specifies how many previously used passwords are acceptable to USM Appliance.	Disabled
Complexity	Specifies that passwords must contain 3 of the following: lowercase characters, uppercase characters, numbers, or special characters.	Disabled
Minimum password lifetime, in minutes	Specifies the minimum amount of time that must pass before a user can change a password again. This option prevents users from changing a new password to the previously expired one.	0 (disabled)
Maximum password lifetime in days	Specifies the number of days before USM Appliance prompts users to change their current password.	0 (disabled)
Failed logon attempts	Number of failed logon attempts before USM Appliance locks an account.	5
Account lockout duration	Amount of time user accounts remain locked.	5 (0 disables lockout)

Configure LDAP in USM Appliance

This topic shows you how to configure USM Appliance to allow user authentication using LDAP, such as Microsoft Active Directory (AD). To create a user for LDAP authentication, see [Create New Accounts for LDAP Users](#).

LDAP (Lightweight Directory Access Protocol) authentication can make user management simpler in larger environments by centralizing user accounts and passwords. For example, LDAP streamlines setting access to various systems and networks based on a user's role. Configuring USM Appliance to use LDAP authenticates users using their standard corporate domain credentials.

Important: LDAP logon names cannot have spaces in the name. Because USM Appliance usernames do not allow for spaces, a space in an LDAP username will not work in USM Appliance.

Creating an LDAP Service Account

To enable USM Appliance to query LDAP for authorization, you must first create a service account in LDAP. For example, in Microsoft Active Directory, you configure an LDAP account as you would a user account.

To create an Active Directory service account

1. Type the name of the person whose account you are setting up, and assign them a user-name for login.
2. Set a logon password, and select Password never expires or the option that best fits your company's or organization's policy.

Important: USM Appliance uses this account to access LDAP each time a user logs in. If the password expires and is not updated in USM Appliance, users will not be able to log in.

New Object - User

Create in: domain1.com/Users

First name: AV Initials: []

Last name: admin

Full name: AV admin

User logon name: AVadmin @domain1.com

User logon name (pre-Windows 2000): DOMAIN1\AVadmin

< Back Next > Cancel

New Object - User

Create in: domain1.com/Users

Password: []

Confirm password: []

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

Configuring USM Appliance to Request Authentication through LDAP

Follow these instructions to configure USM Appliance to request user credential authentication from LDAP, rather than using data stored locally in USM Appliance.

To configure USM Appliance to request LDAP user authentication

1. Log into the USM Appliance web interface and go to **Configuration > Administration > Main**.
2. Click the **Login Methods/Options** section to expand it, and type the required values shown in the [Login Methods/Options Values](#) table.
3. Click **Update Configuration** to save changes.

LOGIN METHODS/OPTIONS ▲		
Setup main login methods/options		
Remote login key	<input type="text"/>	?
Enable LDAP for login	<input type="button" value="Yes"/> ▼	?
LDAP server address	<input type="text" value="127.0.0.1"/>	?
LDAP server port	<input type="text" value="389"/>	?
LDAP server SSL	<input type="button" value="No"/> ▼	?
LDAP server TLS	<input type="button" value="No"/> ▼	?
LDAP server baseDN	<input type="text" value="dc=domain, dc=com"/>	?
LDAP server filter for LDAP users	<input type="text" value="(&(sAMAccountName=%u)(objec"/>	?
LDAP Username	<input type="text" value="admin@domain.com"/>	?
LDAP password for Username	<input type="password" value="....."/>	?
LDAP requires a valid OSSIM user for login	<input type="button" value="Yes"/> ▼	?
Entity for new LDAP user	<input type="text" value=""/>	?
Menus for new LDAP user	<input type="text" value=""/>	?

Login Methods/Options Values

Parameter	Input Value
Remote login key	Required when using remote loggers. Otherwise you can leave it empty. See "Configure the USM Appliance Logger after Deployment" in the <i>USM Appliance Deployment Guide</i> for details.
Enable LDAP for login	Yes
LDAP server address	LDAP server IP address. For example: 127.0.0.1
LDAP server port	389 (unencrypted) or 636 (SSL encrypted)
LDAP server SSL	Yes (Use LDAP server with SSL) or No
LDAP server TLS	Yes (Use LDAP server with TLS) or No
LDAP server baseDN	LDAP server distinguished name (DN) in the format of dc=<domain>,dc=<domain suffix> For instance, if the DN is "example.com", you should enter dc=example,dc=com.
LDAP server filter for LDAP users	General LDAP: (&(cn=%u)(objectClass=account)) Active Directory: (&(sAMAccountName=%u)(objectCategory=person))  Note: To restrict LDAP access to specific users, use the UserAccountControl flags. For example, the entry below allows access to a normal user account: (&(sAMAccountName=%u)(objectCategory=person)(userAccountControl=512)) See Microsoft documentation for additional options.
LDAP Username	User Principal Name (UPN) of the user account in LDAP: <i>loginname@domain.suffix</i>
LDAP password for Username	Password for the account referenced in LDAP Username.

Login Methods/Options Values (Continued)

Parameter	Input Value
Require a valid OSSIM user for login	<p>Yes — Controls user authorization by requiring creation of a user account in the USM Appliance with the same username as in LDAP.</p> <p>No — A local account is not required for initial login. When using this option, the system will automatically create a LDAP enabled local user account using the specified entity assignment and menu template.</p> <p>Local usernames are used to determine user permissions, for example, assigning menu templates and entities. An admin sets a password for the local account during its creation. After LDAP is set up, the local password is no longer used for authentication.</p> <p>If you choose No, you must select a default entity from the Entity for new LDAP user list and a default menu template from the Menus for new LDAP user list. You then assign these to users who are authenticated by LDAP.</p>
Entity for new LDAP user	The default entity assigned to new LDAP users when an OSSIM user is not required.
Menus for new LDAP user	The default menu template assigned to new LDAP users when an OSSIM user is not required.

User Authorization

User Authorization provides methods for limiting user access to different parts of the USM Appliance web interface. This allows the default admin to ensure that only authorized admins can perform specific operations or authorized users can only view specific parts of the UI. Configuring user authorization helps ensure the integrity of USM Appliance by restricting access and operations.

USM Appliance provides the following methods to configure what users can access in USM Appliance:

- **Entity association** — Associates a user with entities within the structure tree. This option is accessible from **Configuration > Administration > Users > Structure**. See [Limit User Visibility with Entities](#) for more information.

- **Allowable assets** — Entity association includes which assets the user is allowed to view. This feature works like a filter within an entity or a correlation context. You can, for this reason, think of it as a subset of entity association (visibility limitation). This option is accessible from **Configuration > Administration > User > New**. See [Create New Accounts for Local Users](#) for instructions.
- **Templates** — Grant access to different parts of the USM Appliance web interface. Templates are a straight forward way of applying or selecting which parts of the UI are accessible to a user. This option is accessible from **Configuration > Administration > Users > Templates**. See [Control User Authorization with Templates](#).

Limit User Visibility with Entities

In USM Appliance, you can limit user access to parts of the web UI by limiting visibility of assets and events with an entity.

USM Appliance uses *entities* to group assets and sensors from similar functional areas of an organization. This allows you to treat some assets differently from others in terms of which users have visibility into them and their events through the web interface. Using this method, you can, for example, limit the users of a given department to see only their department's assets and events.

- If you use local authentication, you can assign an entity to an individual user in USM Appliance. See [Create New Accounts for Local Users](#).
- If you use LDAP authentication without a local user, USM Appliance uses a default entity. See [Create New Accounts for LDAP Users](#).

 **Note:** Visibility configuration does not apply to Availability Monitoring, HIDS, or Vulnerability Scans. Because these functional areas are tied to each USM Appliance Sensor, you cannot limit their visibility to a subset of assets.

For a description of the UI elements on the **Structure** page, see [Entities and Assets Structure Tree Fields](#).

To create a new entity

1. In the USM Appliance web interface, go to **Configuration > Administration > Users > Structure** and click **New Entity**.

The screenshot shows the 'NEW ENTITY' configuration page. It is divided into two main sections: 'GENERAL INFO' and 'SENSORS'/'ASSETS'.

GENERAL INFO:

- Name:** A text input field.
- Address:** A text input field.
- Admin User:** A text input field with the placeholder text 'No users are part of this entity yet...'
- Parent:** A dropdown menu with 'My Company [Context]' selected.
- Timezone:** A dropdown menu with 'Africa/Abidjan' selected.
- SAVE:** A blue button.

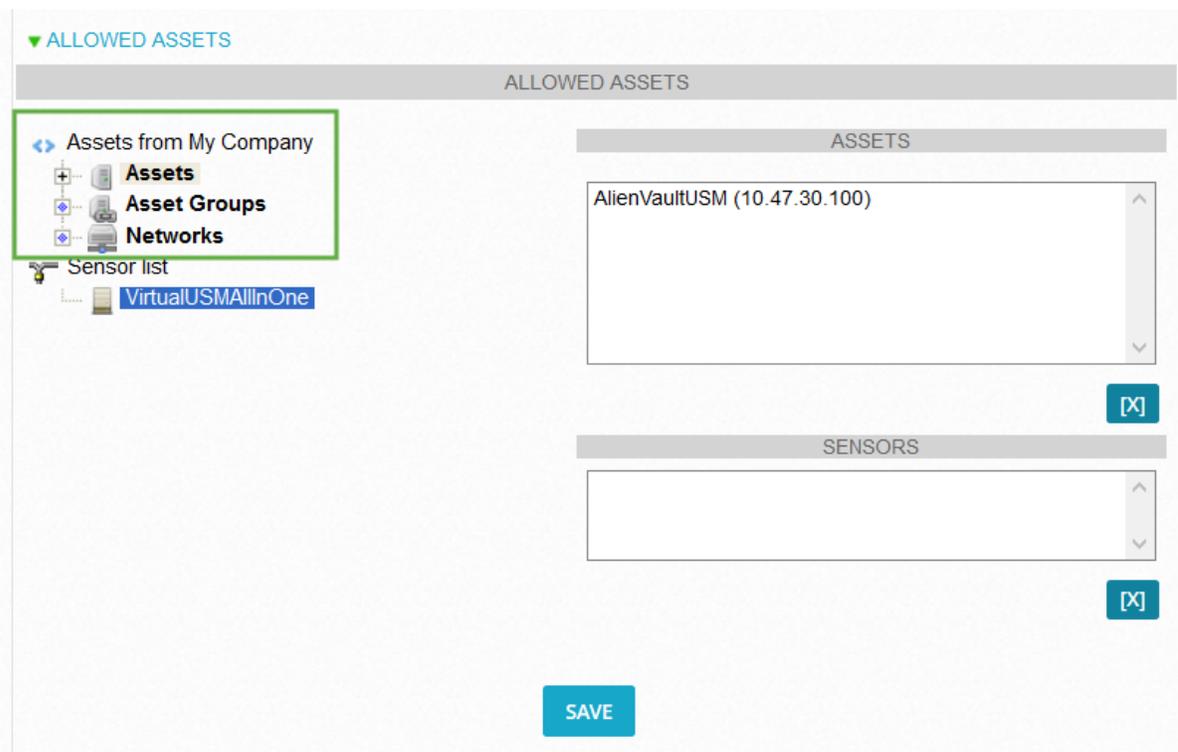
SENSORS:

- A large empty text area for sensor names.
- REMOVE ALL SENSORS:** A blue button with a close icon (X).

ASSETS:

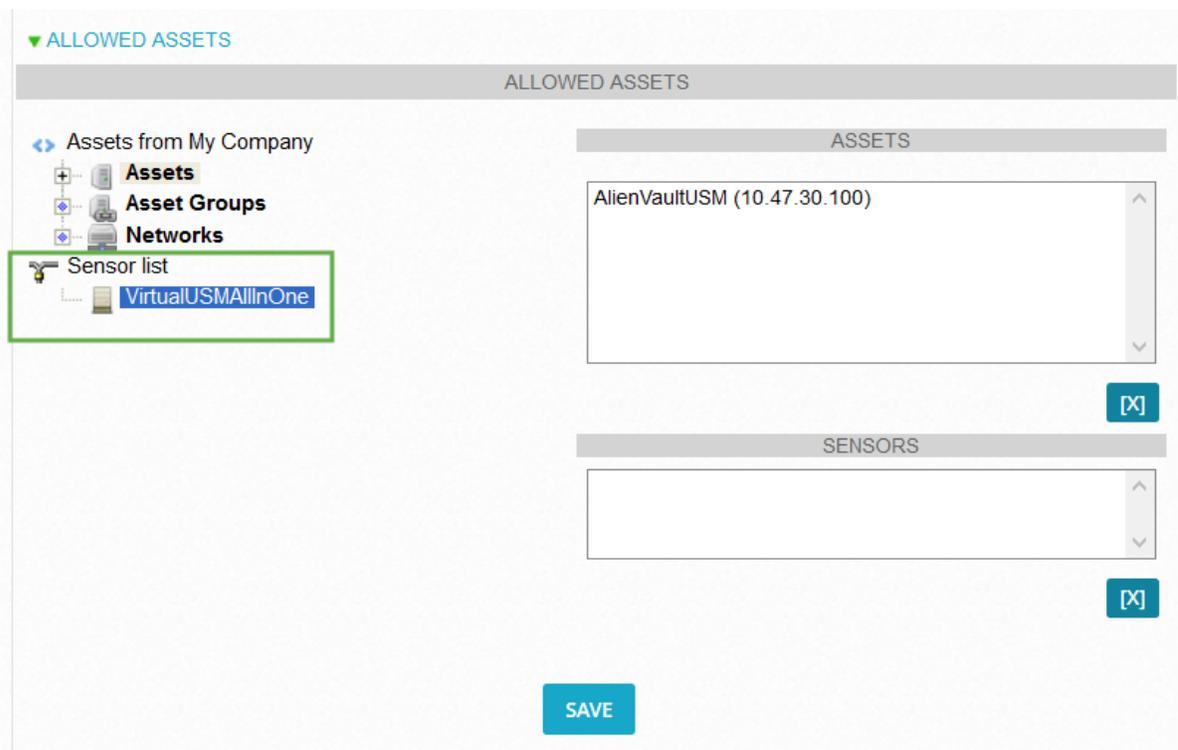
- A large empty text area for asset names.
- REMOVE ALL ASSETS:** A blue button with a close icon (X).
- Filter:** A text input field followed by an **APPLY** button.
- Assets from My Company:** A tree view showing a hierarchy of assets:
 - Assets
 - Asset Groups
 - Networks
 - Network Groups
 - Sensor list
 - VirtualUSMAAllInOne

2. Specify the name of the entity in the **Name** field.
3. (Optional) Specify the address of the entity in the **Address** field.
4. Select a parent correlation context or an entity from the **Parent** list.
5. Select the time zone from the **Timezone** list.
6. Associate assets or networks with the entity by selecting assets or networks from the asset tree.



After you add assets, you can remove them by selecting an asset and clicking the **[X]** button. You can also remove all assets by clicking **Remove All Assets**.

7. Associate a USM Appliance Sensor with the entity by selecting a sensor from the Sensor list tree.



If you change your mind and need to delete a Sensor, click the **[X]** button. You can also remove all Sensors by clicking **Remove All Sensors**.

8. Click **Save**.

Entities and Assets Structure Tree Fields

Use the Entities and Assets Structure tree to create, modify, and delete correlation contexts and entities.

Access the Entities and Assets Structure tree from **Configuration > Administration > Users > Structure**.

ADMINISTRATION

USERS MAIN BACKUPS

USER INFORMATION | ACTIVITY | TEMPLATES | STRUCTURE

ENTITIES & ASSET STRUCTURE Found 1 Entities In The System

New Entity New Correlation Context Show Users Show AlienVault Components

ASSET STRUCTURE

- ↳ All Assets
- ↳ Assets
- ↳ Asset Groups
- ↳ Networks
- ↳ Network Groups
- ↳ Visibility
- ↳ My Company
 - ↳ Assets from My Company
 - ↳ Assets
 - ↳ Asset Groups
 - ↳ Networks
 - ↳ Network Groups

INVENTORY

- ↳ Assets by Property
- ↳ Operating System
- ↳ Users logged
- ↳ Role
- ↳ Department
- ↳ Workgroup
- ↳ Machine state
 - ↳ CPU
 - ↳ Memory
 - ↳ Video
 - ↳ ACL
 - ↳ Route
 - ↳ Storage
 - ↳ Model
- ↳ MAC Address
- ↳ Services
- ↳ Software
- ↳ All hosts

The upper part of the page includes the fields shown in the [Entities and Assets Structure Tree Fields](#) table.

Entities and Assets Structure Tree Fields

Field	Purpose
New Entity	Lets you create a new entity.
New Correlation Context	Lets you create a new correlation context.
Show Users	Toggles the display of users in the entities and asset structure.
Show AlienVault Components	Toggles the display of AlienVault components in the entities and asset structure.

On the lower part of the page, there are two columns.

The left column contains an asset structure tree that displays the following:

- Assets
- Asset groups
- Networks

You organize assets into entities and correlation contexts.

By default, USM Appliance displays one correlation context named **My Company** that contains all assets and networks. There are no default entities.

The right column of the page displays the inventory of all assets, organized by properties. Some examples consist of operating system, role, and department.

Viewing User Hierarchy

USM Appliance offers administrators the ability to review the organization of users within entities and correlation contexts.

To see how users are organized

From the USM Appliance web interface, go to **Configuration > Administration > Users > User Information** and select **Multilevel Tree**, on the far right-side of the page.

LOGIN	NAME	EMAIL	VISIBILITY	STATUS	LANGUAGE
admin	admin	admin@allenvault.com			English
operator	Operator	ops@allenvault.com	My Company	✘	English
user1	user1		My Company	✔	English

User hierarchy

Control User Authorization with Templates

Templates are reusable configurations that allow you to limit user access to parts of the USM Appliance web UI. For example, you might create different templates that give system administrators access to more areas than security engineers.

By creating a template for a group of users, you save yourself time, because the template can be reused for each new user account you create.

When you create user accounts locally in USM Appliance, you can assign a template to an individual user or a group of users with the same USM Appliance responsibilities.

When you use LDAP authenticate users, USM Appliance associates the LDAP users with the default template that's included as part of the original deployment. The default template provides full access with the exception of the part of the UI used to schedule scans.

Templates can make configuring user authorization easier. Depending on your needs, you can do any of the following:

- Use the default USM Appliance template.
- Create a new template for a specific user or group of users.
- Duplicate an existing template and edit as necessary for a specific user or group of users. See [Duplicate a User Account](#) for instructions.

The parameters you can select for designing a template simply represent the different parts of the web UI. Determine which parts of the UI you want a user or group of users to have access to when designing a template.

To create a new template

1. From the USM Appliance web interface, go to **Configuration > Administration > Users > Templates** and click **New**.

2. Specify a name for the template.
3. Select the check boxes for specific pages or activities you want users to have access to.

You can also use the **Select All** or **Unselect All** options to save time.

4. Click **Save Template** or discard the changes by clicking **Cancel**.

For instructions to edit an existing template or create a new template based on an existing template, see [Edit a Template](#).

For instructions to delete a template, see [Delete a Template](#).

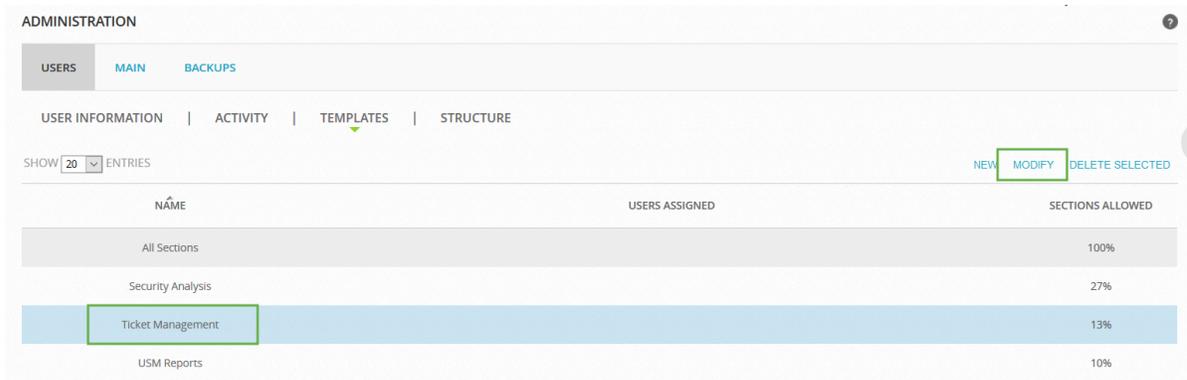
Edit a Template

Use this procedure to either make changes to an existing template or to create a new one by modifying an existing template.

USM Appliance uses one template by default, called **All Sections**. USM Appliance automatically assigns this template to LDAP users, who do not have a local USM Appliance account.

To modify a template

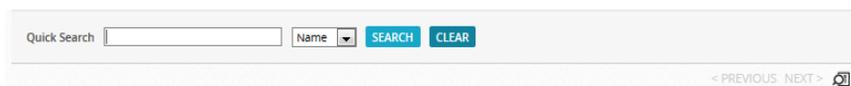
1. From the USM Appliance web interface, go to **Configuration > Administration > Users > Templates**.



NAME	USERS ASSIGNED	SECTIONS ALLOWED
All Sections		100%
Security Analysis		27%
Ticket Management		13%
USM Reports		10%

2. Select the template you want to modify by doing one of following:
 - Click on the row of the template and click **Modify**.
 - Double-click on the row of the template.
 - Click on the name of the template.

To search for templates, you can also click the search icon (🔍).



Quick Search Name

< PREVIOUS NEXT > 🔍

3. Select the check boxes for the menu sections you want to include, or deselect existing selections, to modify the template.

Templates

Field	Description
Action bar	Includes <ul style="list-style-type: none"> • New, Modify, and Delete Selected. • List that allows users to configure the number of displayed templates
Name	Template name.
Users Assigned	Displays which users are assigned to an individual template.
Sections Allowed	Displays the percentage of sections that the system displays in a template.

You can use the **Select/Unselect All** options to select or unselect all web interface sections at the same time.

If you change the template name, the button **Save As** becomes active.

4. Click **Save Changes**, **Save As**, or click **Cancel** to discard the changes.

MODIFY TEMPLATE - TICKET REPORTING

Name: CANCEL SAVE AS SAVE CHANGES

5. Each new template you create displays on the **Configuration > Users > Templates** page.

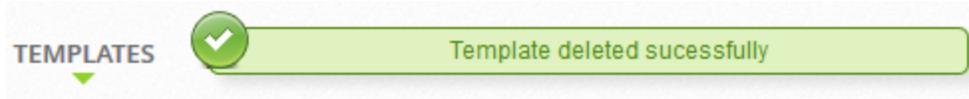
Delete a Template

To delete a template

1. From the USM Appliance web interface, go to **Configuration > Administration > Users > Templates** and place your cursor on the template.
2. Click **Delete Selected**.

3. When prompted whether you really want to delete the template, click **OK**.

A message displays, reporting that the template was successfully deleted.

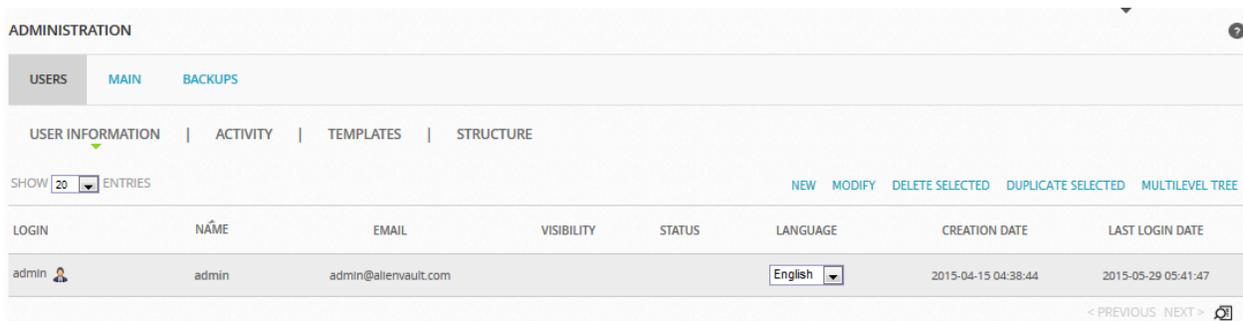


Manage User Accounts

User account management encompasses the tasks administrators perform to create, modify, delete, duplicate, or disable user accounts locally on USM Appliance.

To manage user accounts from the USM Appliance web interface, go to **Configuration > Administration > Users**. The Users page includes the following components:

- An action bar with the options **New**, **Modify**, **Delete Selected**, **Duplicate Selected**, and **Multilevel Tree**, which displays the user accounts in a tree structure.
- A drop-down menu that allows you to configure the number of users to display at one time
- A list of user accounts



User Account Fields

Field	Description
Login	Username required to log into the AlienVault USM Appliance web UI.
Name	The real name of that user in the system.
Email	The email address of the user. It is used to send notifications or reports to the user.
Visibility	The entity the user belongs to.

User Account Fields (Continued)

Field	Description
Status	Indicates whether the user account is enabled or disabled. You can use this field when Enable or Disable a User Account .
Language	The interface is available in either English or Spanish.
Creation Date	Date the user account was created.
Last Login Date	Last date the user logged into the system.

You can also search for templates by clicking the search icon () and specifying the name of the user you are searching for.

Create New Accounts for Local Users

Use this procedure to create new user accounts for local USM Appliance users. For LDAP users, see [Create New Accounts for LDAP Users](#). You must be an admin to create user accounts.

To create a new user account

1. From the USM Appliance web UI, go to **Configuration > Administration > Users > User Information**, and then click **New**.

A form opens for you to enter the user information.

USER LOGIN *	<input type="text"/>		
USER NAME *	<input type="text"/>		
USER EMAIL 	<input type="text"/>		
USER LANGUAGE *	English 		
TIMEZONE *	UTC 		
ENTER YOUR CURRENT PASSWORD *	<input type="password"/>		
ENTER USER PASSWORD *	<input type="password"/>		
RE-ENTER USER PASSWORD *	<input type="password"/>		
ASK TO CHANGE PASSWORD AT NEXT LOGIN	<input type="radio"/> Yes <input checked="" type="radio"/> No		
MAKE THIS USER A GLOBAL ADMIN	<input type="radio"/> Yes <input checked="" type="radio"/> No		
MENU TEMPLATE *	All Sections   		
 Visibility  My Company	<table border="1"> <thead> <tr> <th>VISIBILITY</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> </tr> </tbody> </table> 	VISIBILITY	<input type="text"/>
VISIBILITY			
<input type="text"/>			
▶ ALLOWED ASSETS			
<input type="button" value="SAVE"/>			

2. Fill out the form accordingly.
 - a. **Timezone** is used to display date information in the web UI for alarms, events, raw logs, and reports. The display is user specific.
 - b. In the **Enter Your Current Password** field, type your administrator password.
 - c. In the **Enter User Password** field, type a temporary password for the user.



Important: User passwords must not contain spaces.

- d. In the **Ask to Change Password at Next Login** field, select Yes.
- e. If creating an admin user, select Yes for **Make This User a Global Admin**.
- f. Select a template from the **Menu Template** list.

You can either select an existing template or create a new one from this page. For more information on templates, see [Control User Authorization with Templates](#).

- g. Associate the user with an entity by expanding the **Visibility** structure and click a node. For more information on entities, see [Limit User Visibility with Entities](#).
- h. (Optional) Assign assets that you want this user to see by expanding the **Allowed Assets** option and selecting them.



Important: Menu Templates, Visibility, and Allowed Assets settings do not apply to admin users. You can set them, but they have no effect.

3. Click **Save**.

Create New Accounts for LDAP Users

Use this procedure to create new user accounts for LDAP users. For local users, see [Create New Accounts for Local Users](#). You must be an admin to create user accounts.

Before you can create a user account that uses LDAP authentication, you must first enable LDAP for login. See [Configure LDAP in USM Appliance](#) for instructions.

To create a new LDAP user account

1. From the USM Appliance web UI, go to **Configuration > Administration > Users > User Information**, and then click **New**.

A form opens for you to enter the user information.

USER LOGIN *	<input type="text"/>		
USER NAME *	<input type="text"/>		
USER EMAIL 	<input type="text"/>		
USER LANGUAGE *	English 		
TIMEZONE *	UTC 		
ENTER YOUR CURRENT PASSWORD *	<input type="password"/>		
LOGIN METHOD	LDAP 		
MAKE THIS USER A GLOBAL ADMIN	<input type="radio"/> Yes <input checked="" type="radio"/> No		
MENU TEMPLATE *	All Sections   		
 Visibility  My Company	<table border="1"> <thead> <tr> <th>VISIBILITY</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> </tr> </tbody> </table> 	VISIBILITY	<input type="text"/>
VISIBILITY			
<input type="text"/>			
<p> ALLOWED ASSETS</p>			
<input type="button" value="SAVE"/>			

2. Fill out the form accordingly.
 - a. **Timezone** is used to display date information in the web UI for alarms, events, raw logs, and reports. The display is user specific.
 - b. In the **Enter Your Current Password** field, type your administrator password.
 - c. If you have enabled LDAP, **Login Method** defaults to LDAP.

 **Important:** User passwords must not contain spaces.

- d. If creating an admin user, select Yes for **Make This User a Global Admin**.

- e. Select a template from the **Menu Template** list.

You can either select an existing template or create a new one from this page. For more information on templates, see [Control User Authorization with Templates](#).

- f. Associate the user with an entity by expanding the **Visibility** structure and click a node. For more information on entities, see [Limit User Visibility with Entities](#).
- g. (Optional) Assign assets that you want this user to see by expanding the **Allowed Assets** option and selecting them.



Important: Menu Templates, Visibility, and Allowed Assets settings do not apply to admin users. You can set them, but they have no effect.

3. Click **Save**.

Delete a User Account



Important: Before deleting a user in USM Appliance, check to see if this user has scheduled any vulnerability scans or reports, created any custom reports, or is in charge of any tickets, because they will be deleted as well. If you want to keep any of the scans, reports or tickets, you need to edit them and assign to a different user first.

To delete an existing user account

1. From the USM Appliance web UI, go to **Configuration > Administration > Users > User Information**.
2. Select the user account you want to delete by clicking the row of that user.
3. Click **Delete Selected**.
4. When prompted whether you're sure you want to delete the user, click **OK**.

A message displays, reporting that the user account was successfully removed.

LOGIN	NAME	EMAIL	VISIBILITY	STATUS	LANGUAGE	CREATION DATE	L
admin	admin	admin@alienvault.com			English	2015-10-07 04:21:34	20

Duplicate a User Account

Duplicating an existing user account can save time when you want to create a new user and the new user should have access to most of the same parts of the web interface. For example, you have several employees in the IT group that are responsible for managing USM Appliance tickets. You've already created one user with the appropriate selections for a template, visibility, and assets. Not everything will be identical, of course, but, it often takes less time to deselect a category of authorization than to add many new ones.

To duplicate an existing user account

1. From the USM Appliance web UI, go to **Configuration > Administration > Users > User Information**.
2. Select the user account you want to duplicate by clicking the row of that user.
3. Click **Duplicate Selected**.
4. A new page displays and you will find that USM Appliance appends `_duplicated` to the **User Login** field to highlight that the account is a duplicate.
5. Change any field of the user account as needed.

For instructions to help make changes to the duplicated account, see [Create New Accounts for Local Users](#).

6. Click **Save**.

Modify a User Account

Use this procedure when you want to make modifications to an existing user account.

To modify an existing user account

1. From the USM Appliance web UI, go to **Configuration > Administration > Users > User Information**.
2. Select the user account you want to modify by clicking the row of that user.
3. Click **Modify**.
4. The user account information displays. Change any field of the user account as needed.

For instructions to help make changes to the duplicated account, see [Create New Accounts for Local Users](#).

5. Click **Save**.

Enable or Disable a User Account

User accounts are enabled automatically when they are created. You can disable or enable them again as needed.

To enable or disable a user account

1. From the USM Appliance web UI, go to **Configuration > Administration > Users > User Information**.

2. Select the user account you want to enable/disable by clicking the row of that user.

A green check mark means the account is enabled while a red cross mark means the account is disabled.

3. To disable an account, click the green check mark under the **Status** column.

LOGIN	NAME	EMAIL	VISIBILITY	STATUS	LANGUAGE	CREATION DATE	LAST LOGIN DATE
admin	admin	admin@allenvault.com			English <input type="button" value="v"/>	2015-04-15 04:38:44	2015-05-29 09:03:01
operator	Operator	ops@allenvault.com	My Company		English <input type="button" value="v"/>	2015-05-29 08:30:13	-

Disable account

4. To enable a account, click the red cross mark under the **Status** column.

LOGIN	NAME	EMAIL	VISIBILITY	STATUS	LANGUAGE	CREATION DATE	LAST LOGIN DATE
admin	admin	admin@allenvault.com			English <input type="button" value="v"/>	2015-04-15 04:38:44	2015-05-29 09:03:01
operator	Operator	ops@allenvault.com	My Company		English <input type="button" value="v"/>	2015-05-29 08:30:13	-

Enable account

Reset Password for User Accounts

USM Appliance has specific procedures and permissions for resetting passwords for [different user accounts](#).

User permissions for resetting passwords

User	Can reset password for
Root user	All users
Default admin	Self, admins, and users
Admins	Self, other admins, and users
Users	Self

Reset Password for Admin or Non-admin Users

Follow this procedure to reset password for all web users except for the default admin. Only the default admin can reset password for admin users.

To reset password for web users

1. From the USM Appliance web UI, go to **Configuration > Administration > Users > User Information**.
2. Select the user account you want to modify by clicking the row of that user.
3. Click **Modify**.
4. In the **Enter Your Current Password** field, type your administrator password.
5. In the **Enter User Password** field, type a temporary password for the user.



Important: User passwords must not contain spaces.

6. In the **Ask to Change Password at Next Login** field, select Yes.
7. Click **Save**.

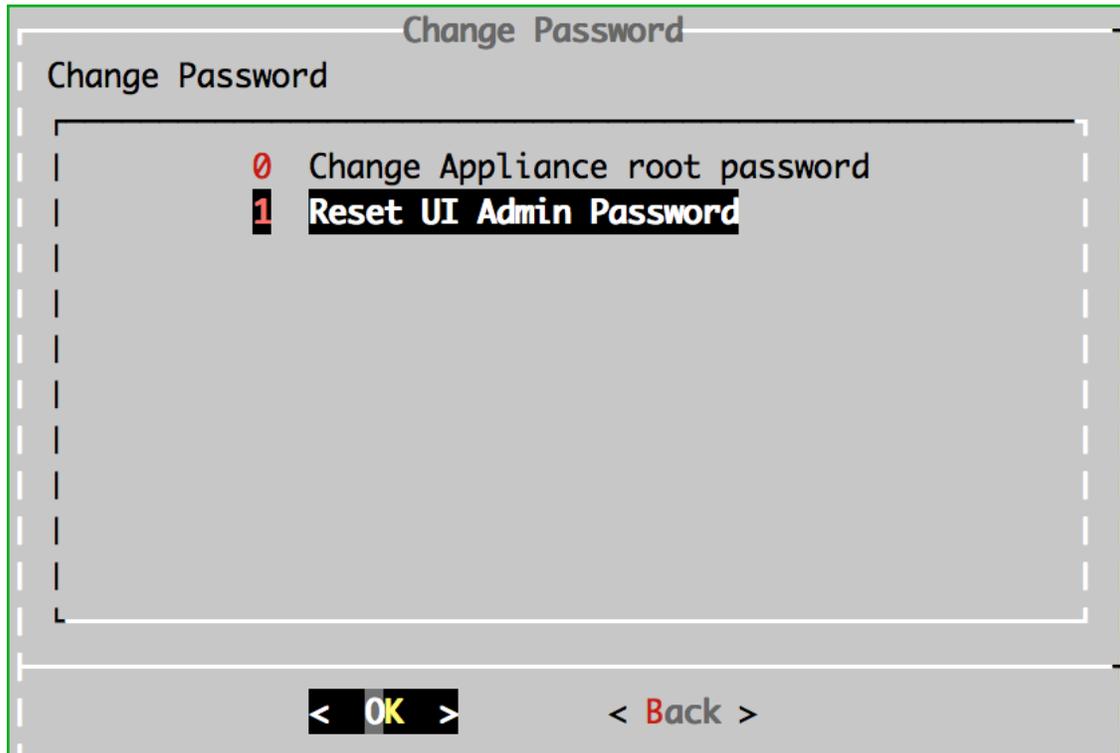
Reset Password for the Default Admin

If the default admin should forget their password, only the AlienVault USM Appliance root user can reset it.

To reset the default admin password

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
2. Select **System Preferences**.
3. Select **Change Password**.

4. Select **Reset UI Admin Password**.



5. Confirm that you want to reset the default admin password by pressing Enter.

The system displays the new password, which you can now give to the default admin.



Note: USM Appliance prompts for a new password when the default admin logs in.

Reset Password for the Root User

If the password for the root user is forgotten or misplaced, and there is only one root user, follow the procedure described in the Knowledge Base article [Recovering Lost Root Password on USM Appliance](#) to reset the password.

If you need to change the password for the root user, follow the steps below.

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.

The AlienVault Setup menu displays.

2. Select **System Preferences**.
3. Select **Change Password**.
4. Select **Change Appliance Root Password**.

5. Confirm that you want to change the root password by pressing Enter.
6. Type a new password and press Enter.
7. Type the password again and press Enter.

Update Your User Profile

All users can update their personal information and password in their own user profile.

To update your account information

1. From the USM Appliance web UI, go to **Settings > My Profile**.

SETTINGS

MY PROFILE CURRENT SESSIONS USER ACTIVITY

USER LOGIN * test3

USER NAME * test3

USER EMAIL ✉

USER LANGUAGE * English

TIMEZONE * UTC

ENTER YOUR CURRENT PASSWORD *

ENTER NEW USER PASSWORD *

RETYPE NEW USER PASSWORD *

SAVE

2. Change your user information or password as needed.
3. Click **Save**.

Monitor User Activities

Every USM Appliance user, regardless of role, has access to the following information:

- **My Profile**

Includes basic settings about a user, such as login name, user name, email, language, time zone, and password. All users can change their profile as described in [Update Your User Profile](#).

- **Current Sessions**

Displays users that are currently logged into the system. Admins (including default admin) can see sessions for all users, while normal users can see only their own account.

SETTINGS ?

MY PROFILE CURRENT SESSIONS USER ACTIVITY

Search:

USERNAME	IP ADDRESS	HOSTNAME	AGENT	LOGON	LAST ACTIVITY	ACTIONS
admin	192.168.73.1	Host-192-168-73-1	Safari 537.36	2018-01-12 17:36:17	0 seconds ago	
test1	192.168.73.1	Host-192-168-73-1	Safari 537.36	2018-01-12 17:35:39	26 seconds ago	

- **User Activity**

Displays user activity. Default admin can see activity of all users, while admins and normal users can only see activity of users belonging to the same entity.

SETTINGS ?

MY PROFILE CURRENT SESSIONS USER ACTIVITY

USER ACTIVITY FILTER

DATE RANGE: - USER: ACTION:

DATE	USER	SOURCE IP	CODE	ACTION
2015-06-01 06:39:44	operator	192.168.250.146	1	User operator logged in
2015-06-01 06:39:38	admin	192.168.250.146	1	User admin logged in
2015-06-01 06:39:35	operator	192.168.250.146	2	User operator logged out
2015-06-01 06:38:54	operator	192.168.250.146	1	User operator logged in
2015-06-01 06:38:46	admin	192.168.250.146	2	User admin logged out
2015-06-01 06:38:41	admin	192.168.250.146	4	Configuration - User operator created
2015-06-01 04:36:04	admin	192.168.250.146	24	Policy - Host: new host added Host:10-47-30-100 [10.47.30.100]

User Activity Configuration

By default, USM Appliance monitors all user activities, including any sessions or configurations created, deleted, or modified by admins or users. This may be helpful for PCI Compliance requirement 10.2.3, Access to all audit trails.

In case you do not want USM Appliance to monitor all user activity, you can fine-tune the user activity parameters.

To review and/or adjust user activity parameters

1. Go to **Configuration > Administration > Main** and expand **User Activity**.

2. Modify the values you want to change. See the table below for reference.
3. Apply your changes by clicking **Update Configuration**.

Configurable Session Parameters

Parameter	Value	Description
Session Timeout (minutes)	Any integer	Configures web session timeout in minutes.  Note: Default is 15 min. 0 means the session does not time out.
User Life Time (days)	Any integer	Configures number of days a user account is active.  Note: Default is blank, or 0 days, which means the account does not expire.
Enable User Log	Yes/No	Controls whether or not user activity should be logged. Default is Yes.
Log to syslog	Yes/No	Determines whether or not to send user activity to syslog. Default is No.

Turning User Activities into Events

If you want to see user activities as events in USM Appliance, AlienVault provides a plugin to turn user activities into events, so that you can manage them together with other security events.

 This feature is only available for USM Appliance All-in-One and USM Appliance Sensor.

To turn user activities in USM Appliance into events

1. In the USM Appliance web UI, go to **Configuration > Administration > Main** and expand **User Activity**.
2. If not already, set **Log to syslog** to Yes.
3. Go to **Configuration > Deployment > Components > AlienVault Center**.
4. Open the instance you want to configure.
5. Click **Sensor Configuration**.
6. Click **Collection**.
7. Select **av-useractivity-syslog** in the Plugins available column and click the plus sign (+) to add it to the Plugins enabled column.

 **Note:** You may see a similar plugin named av-useractivity, which is the predecessor of av-useractivity-syslog and will be deprecated in the future.

8. Click **Apply Changes**.

Events generated by the av-useractivity plugin will now show up as User Activity events under **Analysis > Security Events (SIEM)**.

Using USM Appliance for PCI Compliance

The purpose of this topic is to assist customers in utilizing AlienVault USM Appliance to help achieve Payment Card Industry Data Security Standards (PCI DSS) compliance. Many businesses do not have the tools, knowledge, and resources to fulfill the requirements for PCI Compliance. USM Appliance can play a pivotal role for you by delivering the technologies necessary to achieve PCI compliance.

The PCI DSS are a set of technical and operational requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. Administered by the PCI Security Standards Council, the PCI standard requires validation of compliance on an annual basis.

PCI DSS compliance is a complex process, and the requirements can vary for different organizations, depending on your industry and organization size. You can use the USM Appliance platform's unified approach and built-in essential security capabilities to accelerate and simplify your ability to assess and validate your compliance on critical PCI components. This topic explains which PCI testing procedure that USM Appliance addresses, and how you can use USM Appliance to help you achieve PCI compliance.

- [PCI DSS 3.2 Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data](#)
- [PCI DSS 3.2 Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters](#)
- [PCI DSS 3.2 Requirement 3: Protect Stored Cardholder Data](#)
- [PCI DSS 3.2 Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks](#)
- [PCI DSS 3.2 Requirement 5: Protect All Systems Against Malware and Regularly Update Anti-Virus Software or Programs](#)
- [PCI DSS 3.2 Requirement 6: Develop and Maintain Secure Systems and Applications](#)
- [PCI DSS 3.2 Requirement 7: Restrict Access to Cardholder Data by Business Need to Know](#)
- [PCI DSS 3.2 Requirement 8: Identify and Authenticate Access to System Components](#)
- [PCI DSS 3.2 Requirement 9: Restrict Physical Access to Cardholder Data](#)

- [PCI DSS 3.2 Requirement 10: Track and Monitor Access to All Network Resources and Cardholder Data](#)
- [PCI DSS 3.2 Requirement 11: Regularly Test Security Systems and Processes](#)

Table Legend

Table Headings	Description
Testing Procedure	Description of the PCI Testing Procedure
How USM Appliance Delivers	Explanation of how USM Appliance delivers on this PCI requirement
USM Appliance Instructions	Instructions on how to set up USM Appliance to meet this requirement
USM Appliance Documentation	Link to specific documentation for setting up USM Appliance

PCI DSS 3.2 Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

PCI DSS 3.2 Requirement 1

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.</p>	<p>USM Appliance has built-in reports to assist in identifying changes made to router and firewall configurations for use in validating that changes were approved and tested.</p>	<p>Enable the plugin for your firewall/router devices, and enable forwarding of the syslog events from the firewall/router.</p>	<p>See "Enabling Plugins" in the Plugin Management section of the <i>USM Appliance Deployment Guide</i>.</p>
		<p>Run the existing "Firewall Configuration Change" PCI report to show changes made to the firewall.</p>	<p>How to Run Reports</p>
		<p>Additionally, you can enable instant alerting of suspected device configuration changes by creating a directive to Alert on occurrences of the configuration-change events.</p>	<p>Tutorial: Create a New Directive to Detect DoS Attack</p>

PCI DSS 3.2 Requirement 1 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.</p>	<p>USM Appliance provides NetFlow collection, which assists in identifying insecure services, protocols and ports that are allowed.</p>	<p>NIDS in USM Appliance allows for reporting of suspicious or potentially insecure protocols through events.</p>	<p>See "About AlienVault NIDS" in the IDS Configuration section of the <i>USM Appliance Deployment Guide</i>.</p>
<p>1.3.2 Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.</p>	<p>USM Appliance provides NetFlow collection, which assists in identifying traffic sources and destinations to help ensure that inbound internet traffic is limited to IP addresses within the DMZ.</p>	<p>Create a directive to Alert on occurrences of such NIDS events, which may detect possible misconfiguration or traffic that is not authorized.</p>	<p>Tutorial: Create a New Directive to Detect DoS Attack</p>
<p>1.3.2 Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.</p>	<p>USM Appliance provides NetFlow collection, which assists in identifying traffic sources and destinations to help ensure that inbound internet traffic is limited to IP addresses within the DMZ.</p>	<p>Configure a directive to Alert on any activity from non-authorized networks to the DMZ, which allows for immediate alerting of suspicious traffic from any data source.</p>	<p>Correlation Directives</p>

PCI DSS 3.2 Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

PCI DSS 3.2 Requirement 2

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.1.a Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords have been changed (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings). (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)</p>	<p>In USM Appliance, you can configure a Vulnerability Scan to test for default accounts, passwords and community strings during scans.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Default Accounts 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.1.b For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.</p>	<p>In USM Appliance, you can configure a Vulnerability Scan to test for default accounts, passwords and community strings during scans.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Default Accounts 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.1.1.c Examine vendor documentation and login to wireless devices, with system administrator help, to verify:</p> <ul style="list-style-type: none"> • Default SNMP community strings are not used. • Default passwords/passphrases on access points are not used. 	<p>In USM Appliance, you can configure a Vulnerability Scan to test for default accounts, passwords and community strings during scans.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Default Accounts 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.1.1.e Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.</p>	<p>In USM Appliance, you can configure a Vulnerability Scan to test for default accounts and passwords on wireless devices.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Default Accounts 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry- accepted hardening standards.</p>	<p>In USM Appliance, you can configure a Vulnerability Scan to test for system hardening standards.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the appropriate checks in the scanning profile for the target host.</p>	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.2.d Verify that system configuration standards include the following procedures for all types of system components:</p> <ul style="list-style-type: none"> • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure • Configuring system security parameters to prevent misuse • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. 	<p>The Vulnerability Scan in USM Appliance can assist in testing for system default passwords, detecting running services, and testing system hardening configurations.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Default Accounts ◦ Family: Brute force attacks 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.2.3.a Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols.</p>	<p>The Vulnerability Scan in USM Appliance can assist in identifying insecure services, daemons and protocols.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Service detection ◦ Family: Port scanners ◦ Family: Firewalls ◦ Family: Useless services 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.2.4.b Examine the system configuration standards to verify that common security parameter settings are included.</p>	<p>In USM Appliance, you can configure a Vulnerability Scan to test for system hardening standards.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: General ◦ Family: Compliance 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.2.4.c Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.</p>	<p>In USM Appliance, you can configure a Vulnerability Scan to test for system hardening standards.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: General ◦ Family: Compliance 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.</p>	<p>The Vulnerability Scan in USM Appliance can assist in testing for the presence of Telnet services or other insecure remote-login commands.</p> <p>USM Appliance asset scan discovers open ports and lists them in the inventory.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: General 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 2 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>2.4.a Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each.</p>	<p>USM Appliance has built-in capability for asset management and discovery.</p>	<p>Run an Asset Scan to discover all assets.</p>	<p>Running Asset Scans</p>
		<p>Update and maintain the description field for each asset.</p>	<p>Editing the Assets</p>
		<p>Run the existing Asset Report for an inventory of all assets.</p>	<p>How to Run Reports</p>

PCI DSS 3.2 Requirement 3: Protect Stored Cardholder Data

PCI DSS 3.2 Requirement 3

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>3.4.b Examine several tables or files from a sample of data repositories to verify the PAN (Primary Account Number) is rendered unreadable (that is, not stored in plain-text).</p>	<p>AlienVault NIDS is capable of detecting PAN in NIDS traffic in plaintext, and alerts on it.</p>	<p>Existing correlation directives will generate alarms on credit card information detected in clear text.</p> <p>To verify that credit card data is not being stored in plain text, create a Security Events View with the search on Event Name containing "Credit Card". And then export the view as report module and run the report.</p>	<p>Event Correlation</p> <p>Create Custom Reports from SIEM Events or Raw Logs</p>
<p>3.4.d Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs.</p>	<p>AlienVault NIDS is capable of detecting PAN in NIDS traffic in plaintext, and alerts on it.</p> <p>If a PAN is detected, it is recorded in plaintext in multiple places. It is not automatically removed or otherwise encoded. Manual removal of PAN from logs and DB is required.</p>	<p>Existing correlation directives will generate alarms on credit card information detected in clear text.</p> <p>To verify that credit card data is not being stored in plain text, create a Security Events View with the search on Event Name containing "Credit Card". And then export the view as report module and run the report.</p>	<p>Event Correlation</p> <p>Create Custom Reports from SIEM Events or Raw Logs</p>

PCI DSS 3.2 Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

PCI DSS 3.2 Requirement 4

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>4.1.a Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.</p>	<p>AlienVault NIDS is capable of detecting PAN in NIDS traffic in plaintext, and alerts on it.</p>	<p>Existing correlation directives will generate alarms on credit card information detected in clear text.</p>	<p>Event Correlation</p>
		<p>To verify that credit card data is not being stored in plain text, create a Security Events View with the search on Event Name containing "Credit Card". And then export the view as report module and run the report.</p>	<p>Create Custom Reports from SIEM Events or Raw Logs</p>
<p>4.1.c Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit.</p>	<p>AlienVault NIDS is capable of detecting PAN in NIDS traffic in plaintext, and alerts on it.</p>	<p>Existing correlation directives will generate alarms on credit card information detected in clear text.</p>	<p>Event Correlation</p>
		<p>To verify that credit card data is not being stored in plain text, create a Security Events View with the search on Event Name containing "Credit Card". And then export the view as report module and run the report.</p>	<p>Create Custom Reports from SIEM Events or Raw Logs</p>

PCI DSS 3.2 Requirement 4 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.</p>	<p>USM Appliance can test for the use of insecure versions of SSL and TLS. NIDS data and Vulnerability Scan data combined can assist with this.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: General 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 4 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>4.1.f Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)</p>	<p>The Vulnerability Scan in USM Appliance and AlienVault NIDS can test for the use of insecure versions of SSL and TLS.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: General 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 4 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>4.2.a If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.</p>	<p>AlienVault NIDS is capable of detecting PAN in NIDS traffic in plaintext, and alerts on it.</p>	<p>Existing correlation directives will generate alarms on credit card information detected in clear text.</p>	<p>Event Correlation</p>
		<p>To verify that credit card data is not being stored in plain text, create a Security Events View with the search on Event Name containing "Credit Card". And then export the view as report module and run the report.</p>	<p>Create Custom Reports from SIEM Events or Raw Logs</p>

PCI DSS 3.2 Requirement 5: Protect All Systems Against Malware and Regularly Update Anti-Virus Software or Programs

PCI DSS 3.2 Requirement 5

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.</p>	<p>USM Appliance detects the presence of running processes such as anti-virus software.</p>	<p>Enable the plugin for your anti-virus software, and enable forwarding of the syslog events from the anti-virus manager.</p>	<p>See "Enabling Plugins" in the Plugin Management section of the <i>USM Appliance Deployment Guide</i>.</p>
		<p>Run the anti-virus Raw Logs report to verify the anti-virus software is running.</p>	<p>How to Run Reports</p>
<p>5.2.b Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are</p> <ul style="list-style-type: none"> • Configured to perform automatic updates, and • Configured to perform periodic scans. 	<p>The Vulnerability Scan in USM Appliance can test configurations to make sure that antivirus settings are enabled to perform automatic updates and periodic scans.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Windows 	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>
		<p>View the anti-virus logs in SIEM Events.</p>	<p>Security Events Views</p>

PCI DSS 3.2 Requirement 5 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that</p> <ul style="list-style-type: none"> • The anti-virus software and definitions are current. • Periodic scans are performed. 	<p>The Vulnerability Scan in USM Appliance can test configuration to make sure that antivirus settings are enabled to perform automatic updates and periodic scans.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Windows <p>Run a Vulnerability Scan using the custom scan profile that was created.</p> <p>Export successful scan results and identify findings to determine if system is configured correctly.</p> <p>View the anti-virus logs in SIEM Events.</p>	<p>Creating a Custom Scan Profile</p> <p>Creating Vulnerability Scan Jobs</p> <p>Viewing the Scan Results</p> <p>Security Events Views</p>
<p>5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that</p> <ul style="list-style-type: none"> • Anti-virus software log generation is enabled, and • Logs are retained in accordance with PCI DSS Requirement 10.7. 	<p>USM Appliance detects the presence of running processes such as anti-virus software.</p> <p>USM Appliance also collects and retains logs sent using AlienVault HIDS, in accordance with requirement 5.2.d</p>	<p>Run the anti-virus "Raw Logs" report to verify the anti-virus software is running and generating logs.</p> <p>View the anti-virus logs in SIEM Events.</p>	<p>How to Run Reports</p> <p>Security Events Views</p>

PCI DSS 3.2 Requirement 5 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>5.3.a Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running.</p>	<p>USM Appliance detects the presence of running processes such as anti-virus software.</p>	<p>Run the existing “Antivirus Disabled” PCI report to verify anti-virus software is actively running.</p>	<p>How to Run Reports</p>
<p>5.3.b Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users.</p>	<p>USM Appliance detects the presence of running processes such as anti-virus software.</p>	<p>Run the existing “Antivirus Disabled” PCI report to verify anti-virus software has not been disabled by users.</p>	<p>How to Run Reports</p>

PCI DSS 3.2 Requirement 6: Develop and Maintain Secure Systems and Applications

PCI DSS 3.2 Requirement 6

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>6.2.b For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:</p> <ul style="list-style-type: none"> • That applicable critical vendor-supplied security patches are installed within one month of release. • All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). 	<p>The Vulnerability Scan in USM Appliance can inventory patches and report those that are missing.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Windows ◦ Family: AIX Local Security Checks ◦ Family: Amazon Linux Local Security Checks ◦ Family: CentOS Local Security Checks ◦ Family: Citrix Xenserver Local Security Checks ◦ Family: Debian Local Security Checks ◦ Family: Fedora Local Security Checks ◦ Family: FortiOS Local Security Checks ◦ Family: Free BSD Local Security Checks ◦ Family: Gentoo Local Security Checks ◦ Family: HP-UX Local Security Checks ◦ Family: JunOS Local Security Checks ◦ Family: Mac OSX Local Security Checks ◦ Family: Mandrake Local 	<p>Creating a Custom Scan Profile</p>

PCI DSS 3.2 Requirement 6 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
		Run a Vulnerability Scan using the custom scan profile that was created.	Vulnerability Scans
		Export successful scan results and identify findings to determine if system is configured correctly.	Viewing the Scan Results
<p>6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.</p>	<p>The Vulnerability Scan in USM Appliance provides Web application testing tools.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the following checks in the scanning profile for the target host:</p> <ul style="list-style-type: none"> ◦ Family: Web Application Abuse 	Creating a Custom Scan Profile
		Run a Vulnerability Scan using the custom scan profile that was created.	Vulnerability Scans
		Export successful scan results and identify findings to determine if system is configured correctly.	Viewing the Scan Results

PCI DSS 3.2 Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

PCI DSS 3.2 Requirement 7

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.</p>	<p>USM Appliance can collect security/access logs to provide evidence of access to system components.</p>	<p>Create a directive to Alert on occurrences of successful logins to restricted or limited resources, excluding authorized usernames, which will trigger immediate alarms of possible unauthorized access.</p>	<p>Tutorial: Create a New Directive to Detect DoS Attack</p>

PCI DSS 3.2 Requirement 8: Identify and Authenticate Access to System Components

PCI DSS 3.2 Requirement 8

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>8.1.6.a For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.</p>	<p>In USM Appliance you can view bruteforce logon events to see if they trigger an account lockout, or view account lockout events to see how many times they failed to log on.</p> <p>USM Appliance will generate bruteforce authentication alarms.</p>	<p>Observe USM Appliance bruteforce authentication alarms for notification of login attempts that exceed lockout limitations.</p>	<p>Reviewing Alarms as a List</p>
<p>8.1.7 For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.</p>	<p>In USM Appliance you can view bruteforce logon events to see if they trigger an account lockout, or view account lockout events to see how many times they failed to log on.</p>	<p>USM Appliance detects account lockouts and provides visibility into the next subsequent login to verify that minimum lockout duration is satisfied.</p>	<p>Security Events Views</p>

PCI DSS 3.2 Requirement 8 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>8.5.a For a sample of system components, examine user ID lists to verify the following:</p> <ul style="list-style-type: none"> • Generic user IDs are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used to administer any system components. 	<p>Configure Vulnerability Scans in USM Appliance to test security parameters for Linux and Windows servers.</p>	<p>Create a custom scan profile, and in the "Autoenable plugins option", select the "Autoenable by family" option. Then enable the appropriate checks in scanning profile for target host.</p>	<p>Creating a Custom Scan Profile</p>
		<p>Run a Vulnerability Scan using the custom scan profile that was created.</p>	<p>Vulnerability Scans</p>
		<p>Export successful scan results and identify findings to determine if system is configured correctly.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS 3.2 Requirement 9

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>9.9.1.a Examine the list of devices to verify it includes:</p> <ul style="list-style-type: none"> • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification. 	<p>USM Appliance provides asset management features that can assist in collecting this data.</p>	<p>Run Asset Scan to discover all assets.</p>	<p>Running Asset Scans</p>
		<p>Update and maintain the description and location fields with the appropriate information for each asset.</p>	<p>Viewing Asset Details</p>
		<p>Run the existing Asset Report for an inventory of all assets.</p>	<p>How to Run Reports</p>
		<p>If you find any information outdated or missing, you may edit the asset to enter the appropriate information.</p>	<p>Editing the Assets</p>
<p>9.9.1.b Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date.</p>	<p>USM Appliance provides asset management features that can assist in collecting this data.</p>	<p>Run an Asset Scan to discover all assets.</p>	<p>Running Asset Scans</p>
		<p>Update and maintain the description and location fields with the appropriate information for each asset.</p>	<p>Viewing Asset Details</p>
		<p>Run the existing Asset Report for an inventory of all assets.</p>	<p>How to Run Reports</p>
		<p>If you find any information outdated or missing, you may edit the asset to enter the appropriate information.</p>	<p>Editing the Assets</p>

PCI DSS 3.2 Requirement 10: Track and Monitor Access to All Network Resources and Cardholder Data

PCI DSS 3.2 Requirement 10

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>10.4 Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.</p>	Using Asset Discovery scan in USM Appliance confirms whether NTP is running on server.	Run an Asset Scan to verify presence of NTP service.	Running Asset Scans
<p>10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify:</p> <ul style="list-style-type: none"> • Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. • Systems receive time only from designated central time server(s). 	The Vulnerability Scan in USM Appliance can test system configuration settings to confirm that an NTP server has been configured.	Run a Vulnerability Scan to verify NTP settings are correct.	Vulnerability Scans

PCI DSS 3.2 Requirement 10 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>10.4.2.b Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.</p>	<p>The Vulnerability Scan in USM Appliance can test system configuration settings to confirm that an NTP server has been configured.</p>	<p>Run Vulnerability Scan to verify NTP settings are correct.</p>	<p>Vulnerability Scans</p>
<p>10.5.5 Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.</p>	<p>USM Appliance provides File Integrity Monitoring (FIM) through AlienVault HIDS.</p>	<p>Configure HIDS in USM Appliance to perform File Integrity Monitoring.</p>	<p>File Integrity Monitoring</p>

PCI DSS 3.2 Requirement 11: Regularly Test Security Systems and Processes

PCI DSS 3.2 Requirement 11

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel.</p>	<p>USM Appliance can provide alerting for events that are collected and sent to the SIEM.</p>	<p>Verify that policies, especially those in the "Policies for events generated in server" section, are enabled and configured to use an Action that generates an email to the appropriate contact.</p>	<p>Tutorial: Create a Policy to Send Emails Triggered by Events</p>
<p>11.1.1 Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.</p>	<p>USM Appliance provides asset management features that can assist in collecting this data.</p>	<p>Schedule Asset scans to run regularly in USM Appliance.</p>	<p>Running Asset Scans</p>
		<p>Run the existing Asset Report for an inventory of all assets</p>	<p>How to Run Reports</p>
		<p>If you find any information outdated or missing, you may edit the asset to enter the appropriate information.</p>	<p>Editing the Assets</p>
<p>11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.</p>	<p>Configure Vulnerability Scan in USM Appliance to satisfy this requirement.</p>	<p>See Scan results on Environment > Vulnerabilities > Scan Jobs, and use the Launch Time column to verify dates of scans.</p>	<p>Viewing the Scan Results</p>
<p>11.2.1.b Review the scan reports and verify that the scan process includes rescans until all "high-risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved.</p>	<p>Configure Vulnerability Scan in USM Appliance to satisfy this requirement.</p>	<p>See Scan results on Environment > Vulnerabilities > Scan Jobs, and use the Launch Time column to verify dates of scans.</p>	<p>Viewing the Scan Results</p>

PCI DSS 3.2 Requirement 11 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>11.2.3.b Review scan reports and verify that the scan process includes rescans until:</p> <ul style="list-style-type: none"> • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. • For internal scans, all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. 	<p>Configure Vulnerability Scan in USM Appliance to satisfy this requirement.</p> <p>USM Appliance keeps copies of scans results. Use them to show that ongoing internal scanning is being performed</p>	<p>See Scan results on Environment > Vulnerabilities > Scan Jobs, and use the Launch Time column to verify dates of scans.</p>	<p>Viewing the Scan Results</p>
<p>11.4.a Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic:</p> <ul style="list-style-type: none"> • At the perimeter of the cardholder data environment • At critical points in the cardholder data environment. 	<p>USM Appliance provides NIDS/HIDS functionality and NetFlow information to trace data flow.</p>	<p>From Analysis > Security Events, select “AlienVault NIDS” from the Data Source drop-down. Verify that events are being generated from network traffic that is not local to the USM Appliance device.</p>	<p>Security Events Views</p>
<p>11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion- prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.</p>	<p>USM Appliance provides NIDS/HIDS functionality and NetFlow information to trace data flow.</p>	<p>From Analysis > Security Events, select “AlienVault NIDS” from the Data Source drop-down. Verify that events are being generated from network traffic that is not local to the USM Appliance device.</p>	<p>Security Events Views</p>

PCI DSS 3.2 Requirement 11 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>11.5.a Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:</p> <ul style="list-style-type: none"> • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files • Additional critical files determined by entity (i.e., through risk assessment or other means) 	<p>USM Appliance provides registry integrity monitoring and File Integrity Monitoring (FIM) through AlienVault HIDS.</p>	<p>Create a Security Events view with the search on Event Name containing "integrity" and the data source as "AlienVault HIDS". Then export the view as a report module and run the report.</p>	<p>Create Custom Reports from SIEM Events or Raw Logs</p>
		<p>Additionally, create a directive to Alert on occurrences of HIDS integrity change events, which triggers immediate alarms.</p>	<p>Tutorial: Create a New Directive to Detect DoS Attack</p>
		<p>Examine long term logging on Analysis > Raw Logs by performing a search for any events containing "integrity" and data source as "AlienVault HIDS".</p>	<p>Search Raw Logs</p>

PCI DSS 3.2 Requirement 11 (Continued)

Testing Procedure	How USM Appliance Delivers	USM Appliance Instructions	USM Appliance Documentation
<p>11.5.b Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files, and to perform critical file comparisons at least weekly.</p>	<p>USM Appliance provides File Integrity Monitoring (FIM) through AlienVault HIDS.</p>	<p>Create a Security Events view with the search on Event Name containing "integrity" and the data source as "AlienVault HIDS". Then export the view as a report module and run the report.</p>	<p>Create Custom Reports from SIEM Events or Raw Logs</p>
		<p>Additionally, create a directive to Alert on occurrences of HIDS integrity change events, which triggers immediate alarms.</p>	<p>Tutorial: Create a New Directive to Detect DoS Attack</p>
		<p>Examine long term logging on Analysis > Raw Logs by performing a search for any events containing "integrity" and data source as "AlienVault HIDS".</p>	<p>Search Raw Logs</p>