



USM Appliance™

Deployment 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 May 05, 2023

Contents

System Overview	8
About USM Appliance	9
About USM Appliance System Architecture and Components	16
Event Collection, Processing, and Correlation Workflow	18
USM Appliance Deployments	23
USM Appliance Deployments	24
USM Appliance Deployment Types	25
USM Appliance Deployment Requirements	31
Firewall Permissions	34
Configure the USM Appliance Hardware	37
Deploy USM Appliance in VMware	53
Deploy USM Appliance Using Hyper-V Manager	58
Deploy USM Appliance with AMI	64
Configure the USM Appliance Sensor after Deployment	67
Configure the USM Appliance Logger after Deployment	69
Configure the USM Appliance Enterprise Server and Enterprise Database	74
Set Up the Management Interface	77
Register USM Appliance	79
USM Appliance Initial Setup	83
Access the AlienVault Setup Menu	84
Configure Network Interfaces	86
Configure the Search Domain	89
Configure a Hostname for USM Appliance	90
Change the Default Time Zone	91
Configure USM Appliance to Use a DNS	92
Configure Synchronization with an NTP Server	92

Configure USM Appliance to Recognize Your Local Keyboard	93
Configure Custom HTTPS Certificates in USM Appliance	94
Create the Default Admin User	96
Configure Mail Relay in USM Appliance	97
Configure USM Appliance to Use a Proxy	100
Getting Started Wizard	103
Running the Getting Started Wizard	104
Skipping the Getting Started Wizard	104
Configuring Network Interfaces	105
Discovering Assets in Your Network	108
Deploying HIDS to Servers	112
Enabling Log Management	116
Connecting to AlienVault Open Threat Exchange®	118
IDS Configuration	121
Intrusion Detection Systems	122
AlienVault HIDS	124
AlienVault NIDS	163
VPN Configuration	175
Prerequisites	176
Configure a VPN Between USM Appliance Systems	176
Building a VPN Tunnel Without a Client-Server Connection	180
Verifying the VPN Connection	183
Disabling a VPN Configuration	183
High Availability Configuration	185
How Does the High Availability Solution Work?	186
High Availability Prerequisites and Restrictions	187
Configuring High Availability in USM Appliance Standard Systems	189
Configuring High Availability in USM Appliance Enterprise Systems	202

Disabling High Availability	206
Upgrading a USM Appliance Deployment Configured for High Availability	207
Plugin Management	210
Plugin Fundamentals	211
Enable Plugins	227
Configure Plugins	237
Customize and Develop New Plugins	258
Update Process	284
USM Appliance Updates	285
Update USM Appliance Online	286
Update USM Appliance Offline	290
Operating System Upgrade in Version 5.8.0	295
Error Codes When Updating from Version 5.8.0 to Version 5.8.x	299
Backup and Restoration	304
Back Up and Restore Alarms	305
Back Up and Restore Events	308
Back Up and Restore MongoDB	311
Back Up and Restore NetFlow Data	313
Back Up and Restore Raw Logs	316
Back Up and Restore System Configuration	319
Migrate Your USM Appliance Deployment	327
Restore Software on a USM Appliance Hardware	333
Update Your AlienVault License Key	339
System Maintenance and Remote Support	342
Message Center	343
Remote Support	348
Locate the AlienVault License and System ID	352
Purge Old System Logs	353

Replace Disk Drives or Power Supplies	354
---	-----

System Overview

This is a basic overview of AlienVault USM Appliance as it is deployed and used in your environment. Individual subjects covered in the System Overview include the following:

- [About USM Appliance](#) — describes current risks in the business environment due to security threats and vulnerabilities, the role of risk assessment, an overview of USM Appliance security management capabilities for organizations to assess and mitigate risks, to detect threats and prioritize response, and to achieve compliance.
- [About USM Appliance System Architecture and Components](#) — provides description of the USM Appliance architecture, including major system components and functionality.
- [USM Appliance Deployments](#) — provides description of best practices for installation and configuration of USM Appliance.
- [Event Collection, Processing, and Correlation Workflow](#) — describes the overall USM Appliance workflow, from collection of raw log data from networked devices to analyzing and determining risk from various threats and vulnerabilities.

About USM Appliance

Businesses today are exposed to an ever-increasing number of threats:

- Network-based threats — Aimed at networks and network infrastructure.
- Host-based threats — Aimed at individual hosts.
- External threats — Coming from external attackers.
- Internal threats — Coming from internal attackers.

Although the goal of security solutions is to detect and prevent such threats, no network can be completely protected from them all. For this reason, USM Appliance focuses on mitigating risk, identifying vulnerabilities, detecting threats, and prioritizing response to the highest priority threats and vulnerabilities. Measures for mitigating risk, identifying vulnerabilities, and detecting threats include the following:

- Identifying patterns of events that indicate a possible threat or vulnerability.
- Determining the risk of potentially harmful attacks or compromise.
- Implementing controls to address reported vulnerabilities.
- Taking action to respond to identified attacks.
- Performing ongoing monitoring and reporting of network and host-based activities.

The Role of Risk Assessment

To properly secure your infrastructure, first conduct a risk assessment of your assets. Risk assessment helps you determine the relative importance of the assets within your network, the vulnerabilities of those assets in relation to specific exploitation threats, and the likelihood of security events taking place against those assets. After completing these analyses, you can design security policies in response to the relative asset values and exploitation risks that various threats and vulnerabilities pose.

Strong security policies focus on how best to protect your most vital and at-risk assets. For example, if a network resource is critical and the likelihood of an attack against it is high, focus your efforts on creating security policies that monitor for such attacks, and develop response plans to them.

How USM Appliance Helps with Risk Assessment and Mitigation

USM Appliance provides you with the ability to identify your critical assets and to set policies to alert you when those assets have vulnerabilities or are subjected to attacks. USM Appliance will generate alarms based upon the risk associated with any given security event captured in USM Appliance.

The importance given to any given security event depends on three factors:

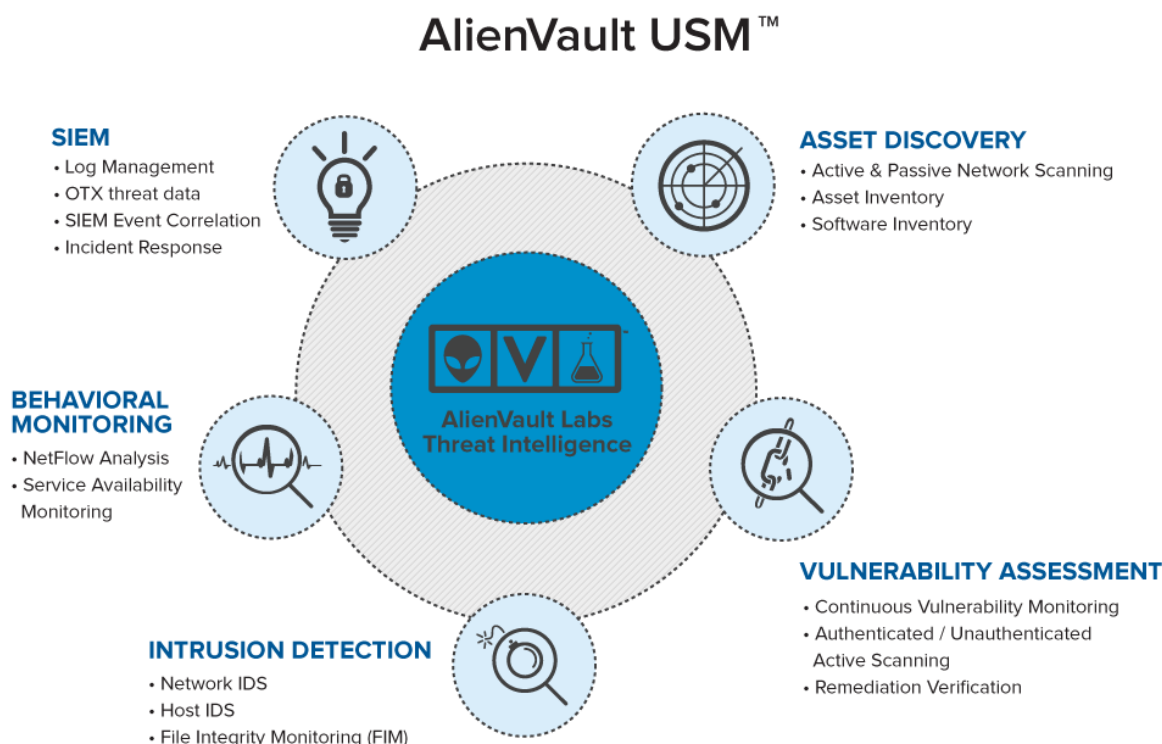
- The value of the asset associated with the event
- The threat represented by the event
- The probability that the event will occur

These factors are the building blocks for the traditional definition of risk: a measure of the potential impact of a threat on your assets and the probability a threat will be carried out.

Each event generated in USM Appliance is evaluated in relation to its associated risk; in other words, in proportion to the assets at risk, the threat represented by the event, and the probability the threat is real. Accordingly, USM Appliance provides you the capability to identify all high risk events, some of which will result in alarms, and allow you to properly prioritize your response.

How USM Appliance Helps Detect Threats and Prioritize Responses

The following illustration highlights the capabilities and related tools that USM Appliance provides to help you perform security management tasks in your own environment.



Asset Discovery — Combines core discovery and inventory technologies to give you visibility into the devices that are on your network. Features include:

- Active and Passive Network Scanning
- Asset Inventory
- Service Inventory

Performing asset discovery and inventory are the first essential steps to knowing what systems and devices are on your network. USM Appliance combines core discovery and inventory technologies to give you visibility into the devices you want to monitor.

Note: Before scanning a public network space, see [Addendum Notice Regarding Scanning Leased or Public Address Space](#).

Vulnerability Assessment — Identifies assets and devices with unpatched software, insecure configurations, and other vulnerabilities on your network. Features include:

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning
- Remediation Verification

The integrated internal vulnerability scanning keeps you abreast of vulnerabilities on your network, so you can prioritize patch deployment and remediation. Continuous correlation of your dynamic asset inventory with our vulnerability database provides you with up-to-date information on the vulnerabilities in your network, in-between your scheduled scans.



Note: Before scanning a public network space, see [Addendum Notice Regarding Scanning Leased or Public Address Space](#).

Intrusion Detection — Coordinates incident response and threat management across your network with built-in security monitoring technologies, emerging threat intelligence from AT&T Alien Labs™, and seamless closed-loop workflow for rapid remediation. Features include:

- Network-based IDS (NIDS)
- Host-based IDS (HIDS)
- File Integrity Monitoring (FIM)

Built-in file integrity monitoring in host-based agents installed on servers alerts you to unauthorized modification of system files, configuration files or content. Monitoring of network access using host- and network-based detection systems identifies who tried to access those systems, files, and content.

Behavioral Monitoring — Identifies anomalies and other patterns that signal new, unknown threats in your network, as well as suspicious behavior and policy violations by authorized users and devices. Features include:

- NetFlow Analysis
- Service Availability Monitoring
- Network Protocol Analysis / Packet Capture

Integrated behavioral monitoring gathers data to help you understand “normal” system and network activity, which simplifies incident response when investigating a suspicious operational issue or potential security incident. Full packet capture enables complete protocol analysis of network traffic, providing a comprehensive replay of the event that occurred during a potential breach.

Security Information and Event Management (SIEM) — Identify, contain, and remediate threats in your network by prioritizing your risk and response. Features include:

- Log Management
- Integrated OTX Threat Data
- SIEM Event Correlation
- Incident Response

You can automatically correlate log data with actionable security intelligence to identify policy violations and receive contextually relevant and workflow-driven response procedures. You can also conduct forensic analysis of events using digitally signed raw logs. The raw logs also can be used to satisfy compliance requirements for evidence preservation.

A web-based user interface provides access to all the security management functions provided by AlienVault USM Appliance. The *USM Appliance User Guide* provides information on accessing and using all of the tools in USM Appliance and performing specific security management operations from this user interface.

Managing Regulatory Compliance in USM Appliance

In addition to regular security management operations, USM Appliance also delivers essential security capabilities to help you achieve regulatory compliance. Through its built-in asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, log management, and file integrity monitoring, USM Appliance can help organizations achieve compliance with regulations such as PCI DSS, GLBA, ISO/IEC 27001, FISMA, NERC CIP, FERPA, and SOX. USM Appliance also generates built-in reports specifically for HIPAA, PCI, GLBA, ISO 27001, FISMA, NERC CIP, GPG13, and SOX.

In addition, the "Using USM Appliance for PCI Compliance" section in the *USM Appliance User Guide* provides detailed information on using USM Appliance to help achieve PCI DSS compliance. This information can also be useful in meeting compliance regulations for other standards as well.

About AlienVault Threat Intelligence

AlienVault Threat Intelligence, integrated into USM Appliance through the Threat Intelligence Subscription, provides USM Appliance with capabilities that differentiate it from most other security management solutions available in the marketplace today. AlienVault Threat Intelligence, developed by the AT&T Alien Labs™ Security Research Team and powered by the AT&T Alien Labs™ Open Threat Exchange® (OTX™), is actionable information about the threats facing your network, including the malicious actors, their tools, their infrastructure, and their methods. AlienVault Threat Intelligence tells you what the threat is, where it's originating from, which assets in your environment are at risk, and how to respond.

Alien Labs

Alien Labs is an internal security research team at AT&T Cybersecurity, consisting of security experts who perform ongoing research and analysis of emerging global threats and vulnerabilities. This team constantly monitors, analyzes, reverse-engineers, and reports on sophisticated zero-day threats, including malware, botnets, and phishing campaigns.

The team regularly publishes threat intelligence updates to the USM Appliance platform in the form of correlation directives, IDS signatures, vulnerability signatures, asset discovery signatures, IP reputation data, data source plugins, and report templates. The team also provides up-to-the-minute guidance on emerging threats and context-specific remediation guidance, which accelerates and simplifies threat detection and response.

The Alien Labs team also leverages the collective resources of OTX, the world's largest crowd-sourced repository of threat data to provide global insight into attack trends and malicious actors. The security experts at AT&T Cybersecurity analyze, validate, and curate the global threat data collected by the OTX community.

The Security Research Team improves the efficiency of any security monitoring program by delivering the threat intelligence necessary to understand and address the most critical issues in your networks. They perform the analysis, allowing you to spend your scarce time remediating and mitigating the threats, rather than researching them.

Open Threat Exchange®

The Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network. OTX provides open access to a global community of threat researchers and security professionals. It now has more than 100,000 participants worldwide, who contribute over 19 million threat indicators daily. It delivers community-generated threat data and OTX *pulses*, enables collaborative research, and automates the process of updating your security infrastructure with threat data from any source. OTX enables anyone in the security community to actively discuss, research, validate, and share the latest threat data, trends, and techniques, strengthening your defenses while helping others do the same.

The OTX community and corresponding threat data is one of the critical data sources used by the Alien Labs team to generate AlienVault Threat Intelligence. Alien Labs leverages the collective resources of the OTX by analyzing, validating, and curating the global threat data contributed by the OTX community.



AlienVault OSSIM Limitations: AlienVault OSSIM doesn't include the USM Appliance Logger.

Unauthorized Modification of USM Appliance Can Lead to Instability

AlienVault USM Appliance are built to provide customers with an easy-to-use solution to help monitor the security of their infrastructures. They are delivered in three form factors:

- Hardware appliances,
- Virtual appliances, and
- Amazon appliances.

These appliances include the AlienVault operating system and USM Appliance software necessary to provide the built-in Unified Security Management® (USM) security capabilities.

The appliances include an option to access the CLI of the appliance from the AlienVault Console. This is done by selecting the "Jailbreak System" option from the AlienVault Setup menu, which provides limited shell access to the appliance. This option is available to help customers troubleshoot network issues, data collection issues, and to help the AlienVault Support team work with you to resolve any issues you encounter with the product while working on a support case.

As per the [AlienVault Terms and Conditions](#), AlienVault does not allow modification of system level configuration files, database, or the underlying tools used to provide the functional capabilities offered by the product. Although AlienVault has integrated various open source tools, the configurations used by USM Appliance are designed to provide explicit functionality as described in the product documentation. Changes made to the operating system, tool configurations, or software can destabilize the appliance and prevent the appliance from working properly.

Modifications to the operating system, tool configurations, or software may lead to instability, thus require a reset of the appliance to factory settings to resolve it. AlienVault discourages customers from making such modifications. If there is a use case that requires you to jailbreak the device, we encourage you to share with us the details of the use case and we will consider the idea for a future release of the product.

Our goal is to provide a simple, stable, easy-to-use security platform to help you monitor your environment for threats. Keeping the system stable and free from such modifications will prevent unnecessary downtime, performance issues, and maintenance.

If you have any questions, please contact [AT&T Cybersecurity Technical Support](#).

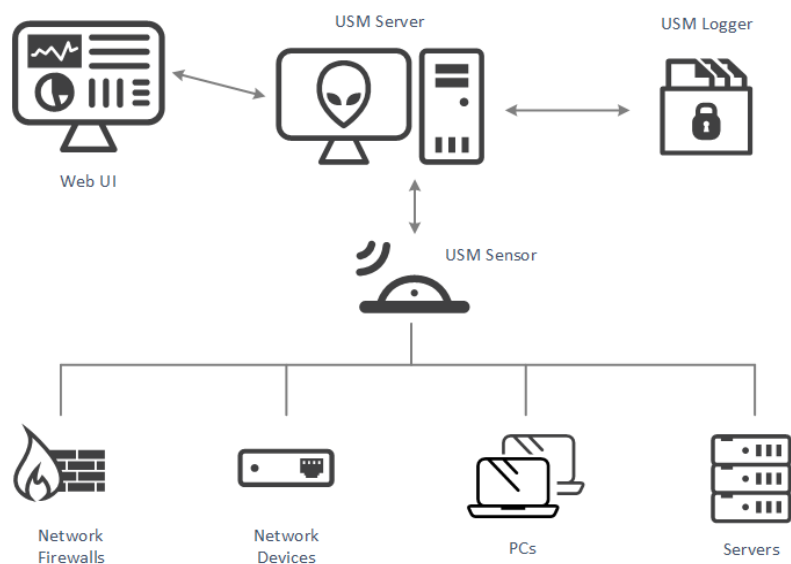
Addendum Notice Regarding Scanning Leased or Public Address Space

AlienVault USM Appliance and AlienVault OSSIM® contain a number of built-in tools for asset and network discovery, enumeration, and vulnerability scanning. These tools utilize various methods for discovery, often by mimicking the behavior of the traffic which they are attempting to protect you from in order to ascertain your exposure to such traffic. This leaves the potential for legitimate scans to be misinterpreted as malicious traffic.

In an effort to combat malicious behavior on the internet, several internet service providers and hosting providers have added scanning restrictions in their contracts. And a number of countries have written laws regarding these practices. In many cases, the response for violation of these rules may range from a written warning to contract cancellation and even civil or criminal charges. As a result, it is very important to check with your internet service providers, hosting providers, and local government to establish any legal or contractual restrictions before attempting to scan hosts or networks outside of your internal network space.

About USM Appliance System Architecture and Components

As a unified security platform, USM Appliance combines several critical security technologies in one integrated platform. USM Appliance can be deployed as a single appliance or distributed across multiple servers (either virtual or hardware) to provide additional scalability and availability. The following figure presents a high-level overview of the AlienVault USM Appliance system architecture.



The three components of the USM Appliance architecture that work together to monitor and provide security in your environment are

- USM Appliance Sensor(s) — Deployed throughout the network to collect and normalize information from any devices in your network environment that you want to manage with USM Appliance. A wide range of plugins are available to process raw logs and data from various types of devices such as firewalls, routers, and host servers.
- USM Appliance Server — Aggregates and correlates information that the USM Appliance Sensors gather. (This is USM Appliance's SIEM capability.) Provides single pane-of-glass management, reporting, and administration through a web-based user interface.
- USM Appliance Logger — Securely archives raw event log data for forensic research and compliance mandates. (This archive of raw event data is also referred to as cold storage.)

Basic USM Appliance Workflow

There is a consistent workflow that USM Appliance follows in collecting raw data from network devices, then parsing and normalizing that data into a stream of events which can then be stored, filtered, and correlated to identify threats and vulnerabilities.

1. USM Appliance Sensors passively collect logs and mirrored traffic, and actively probe assets in the network, to obtain information about the current network activity going on in your environment..
2. The USM Appliance Sensor parses the raw data from different sources and transforms it into a stream of events, each having a common set of data fields. It then sends the events to the USM Appliance Server.
3. The USM Appliance Server correlates the events and assesses their risk.
4. The USM Appliance Server sends the events to the USM Appliance Logger, which signs them digitally and stores them for forensic analyses, archival, and regulatory compliance.

For a more in-depth description of event collection and processing, see [Log Collection and Normalization in USM Appliance](#). Also refer to the "About the Use of Policies in USM Appliance" and "About Correlation" topics in the *USM Appliance User Guide*.

USM Appliance Deployment Options

AlienVault USM Appliance can be deployed in one of two basic configurations:

- Simple Deployment Model — All USM Appliance components (Sensor, Server, and Logger) are combined in a USM Appliance All-in-One appliance. This configuration is most often used in smaller environments, as well as for demonstrations and proof-of-concept deployments.
- Multi-tier, Distributed Deployment Model — This model deploys each AlienVault USM Appliance component (Sensor, Server, and Logger) as an individual virtual or hardware appliance to create a distributed system topology.

The distributed deployment model also comes in two versions, USM Appliance Standard and USM Appliance Enterprise, that increase scalability and performance by provisioning dedicated systems for each USM Appliance component. See [USM Appliance Deployment Examples](#) for more details on USM Appliance deployment models and examples.



AlienVault OSSIM Limitations: AlienVault OSSIM doesn't include the USM Appliance Logger.

Event Collection, Processing, and Correlation Workflow

All AlienVault USM Appliance's security monitoring and management capabilities stem from its overall ability to collect data from devices, transform the data into a common set of data fields that define events, and then process, filter, and correlate those events to identify potential threats and vulnerabilities, or real occurrences of attacks. USM Appliance also assesses the importance and priority of events by assigning risk values based on the value of the underlying assets, the source and nature of the identified threat, and the likelihood of successful attack. More detail on this overall workflow is provided in this section for the following topics:

- Log Data Collection, Parsing, and Normalization
- Event Processing and Filtering
- Event Correlation, Alarms, and Notification
- Event Visualization and Analysis

Log Data Collection, Parsing, and Normalization

Log collection is at the root of AlienVault security management. AlienVault USM Appliance collects logs from various sources: network devices, such as firewalls and routers, host servers and systems, and software applications running on servers. Some devices, for example, those that support the Syslog protocol, are configured to send their logs directly to the USM Appliance Sensor. For other devices, USM Appliance goes out and retrieves the logs. In both cases, data in the logs is normalized to extract and store information in common data

fields that define an event: IP addresses, host names, user names, interface names, and so on. These are the events that a security analyst can analyze in USM Appliance to uncover threats and vulnerabilities, and assess an organization's risk.

Log Parsing Using Plugins

Running on a USM Appliance Sensor, an AlienVault USM Appliance agent is configured with a collection of different log-parsing plugins, which define how to collect logs from specific devices, systems, or applications, and how to transform that log data into standardized event data fields before sending the events to the USM Appliance Server. The plugins also control other event-gathering functions on the sensor, such as intrusion detection. USM Appliance comes equipped with plugins for many commonly encountered data sources. Contact AlienVault to request a new plugin for any data source or product for which a plugin does not already exist. You can also create your own custom plugins, or customize USM Appliance's existing plugins.

Normalization of Security Events

No matter the format of a log message, certain pieces of data (such as user names or IP and MAC addresses) are common in all of the device logs. Extracting these values out of the log message text and storing them into matching common fields is called *normalization*. Normalization is what allows you to perform queries across events collected from varied sources (for example, "Show all events where the source IP is 192.168.1.3".) Although the format of the original data collected from devices may be different, similar information across devices is stored in the same field for events sent to the USM Appliance Server.

The logs are broken down into their message type, and the information from them is used to populate a standard set of fields that define an event (for example, date, sensor, plugin_id, priority, src_ip, src_port, dst_ip, dst_port, username, userdata1).



Note: For a complete list of normalized event fields, see "Event Details – Fields" in the *USM Appliance User Guide*.

Event Processing and Filtering

After normalizing the data obtained from log files and other sources, the USM Appliance Sensor transmits security events to the USM Appliance Server. The USM Appliance Server also performs several additional operations on incoming events, including:

- Parsing the event priority and reliability — Each event type is assigned a priority, which indicates how urgently the event should be investigated, and a reliability score, which assesses the chance the event is a false positive.
- Checking asset values to calculate a risk score — The USM Appliance Server maintains an inventory of known devices on the network, with an associated asset value for each device, defining their importance to the organization. This asset value is then weighed against the event's priority and reliability score to produce a risk value. Higher risk scores help analysts know what is most important to examine first.

For more information on how USM Appliance calculates risk, see "USM Appliance Network Security Concepts and Terminology" in the *USM Appliance User Guide*.

- Application of the event taxonomy — There are system and network events common across many system types, no matter the source of the event or its original data format. AlienVault maintains a hierarchical categorization of event types (referred to as a taxonomy) to which USM Appliance can match events in policies and correlation directives.
- Cross-checking reputation data — The USM Appliance Server checks the IP addresses specific to each event against a reputation database of Internet addresses. IP addresses that match are flagged for future reference and follow-up.

After performing these operations, and based on specified user policy and filter conditions, the USM Appliance Server will save selected or qualified events in a SIEM events database for further analysis and correlation. The events database commonly resides on the same host as the USM Appliance Server, but in large deployments, the database can be installed on a separate host for increased performance and capacity.

Event Correlation, Alarms, and Notification

Following the basic processing, analysis, and filtering that the USM Appliance Server performs, selected or qualified events are fed into the AlienVault USM Appliance correlation engine. Using AlienVault USM Appliance correlation, analysts can look for patterns and sequences of events across multiple devices and system types. Events may actually be processed by the correlation engine several times, as different correlation rules may take the same events as input.

Correlation directives create alarms

As events continue to feed into the correlation engine, USM Appliance generates alarms based on event conditions specified in correlation directives or rules:

- Alarm processing starts when the conditions of a correlation directive are met.
- Alarms may trigger on a single event matching certain conditions, or may require a specific sequence of events to trigger.
- Alarm processing may continue over a matter of hours. Alarms that appear in the system may indicate they are still processing additional incoming events to further corroborate detection.
- Alarms are themselves events (directive events), that can feed into other correlation directives once they are triggered, so you can create cascading levels of alarms.

In addition, when you sign up for the Open Threat Exchange® (OTX™), USM Appliance is configured to receive raw “pulse” data and indicators of compromise (IoCs), from OTX. USM Appliance correlates that data and alerts you to any related OTX pulse and IP reputation-related security events and alarms when it detects those same IoCs interacting with assets in your environment.

As soon as you log into USM Appliance, you can see from the USM Appliance dashboard which OTX indicators are active in your environment. You will receive immediate notification in the form of an event or an alarm when a malicious IP address identified in OTX communicates with any of your system assets, or when USM Appliance identifies any other IoCs seen in OTX are active in your network.



Note: For more information about how USM Appliance alarms are processed and correlated, see "Alarm Management" in the *USM Appliance User Guide*.

Event Visualization and Analysis

Events obtained from device logs, as well as those generated by the correlation engine itself, can all be searched, viewed, and reported on from the USM Appliance web UI. Two different options are available to access and view events:

- View of security events with options to search, filter, and group events based on specific event field values. To use this option, select **Analysis > Security Events** (SIEM) from the web UI.
- View of raw log events displayed with a specific time frame. To use this option, select **Analysis > Raw Events** from the web UI.

For more information on viewing events and performing other security management operations from the USM Appliance web UI, see "Reviewing Security Events (SIEM)" and "Reviewing the Raw Logs" in the *USM Appliance User Guide*.

USM Appliance Deployments

USM Appliance is designed to provide an easy-to-deploy and easy-to-operate security management solution. It is particularly well suited for small-to-medium sized businesses who, similar to larger enterprises, need to ensure the security of their network environment, but may not have as large a support staff to set up and manage more complex security management systems.

Topics covered in this section include the following:

USM Appliance Deployments	24
USM Appliance Deployment Types	25
USM Appliance Deployment Requirements	31
Firewall Permissions	34
Configure the USM Appliance Hardware	37
Deploy USM Appliance in VMware	53
Deploy USM Appliance Using Hyper-V Manager	58
Deploy USM Appliance with AMI	64
Configure the USM Appliance Sensor after Deployment	67
Configure the USM Appliance Logger after Deployment	69
Configure the USM Appliance Enterprise Server and Enterprise Database	74

USM Appliance Deployments

USM Appliance is designed to provide an easy-to-deploy and easy-to-operate security management solution. It is particularly well suited for small-to-medium sized businesses who, similar to larger enterprises, need to ensure the security of their network environment, but may not have as large a support staff to set up and manage more complex security management systems.

In addition to being easier to set up and operate than most alternative systems, USM Appliance also has a modular architecture that provides flexibility in configuring both performance and capacity. The USM Appliance All-in-One combines all components of the USM Appliance solution in a single virtual or hardware machine. In addition, based on the present or future needs of your specific environment, you can also scale individual components in the USM Appliance architecture to run on dedicated machines, add sensors to collect logs from more devices and networks, and implement other features such as high availability, monitoring of devices on remote networks, and remote management of USM Appliance.



Note: For more information and a summary of deployment and configuration options, refer to [USM Appliance Deployment Types](#). This section also provides examples of different size and scale deployment configurations of USM Appliance.

Deployment Sizing and Scaling

There are numerous factors that can influence your USM Appliance configuration and the specific USM Appliance architecture you choose to deploy. The principal factor is the number of events per second that the devices in your environment might be expected to produce. In estimating the total volume of events, you need to include all devices in your environment that you want to monitor and manage with USM Appliance (including firewalls, routers, and host servers, as well as installed applications) and estimate the aggregate activity on these devices.

In addition, you may need to consider other aspects of the specific security management use cases you plan to address with your USM Appliance deployment, which may include but is not limited to

- Specific regulatory compliance requirements you may have
- Number and different types of devices you want to monitor
- Number of users of your systems
- Specific requirements for event correlation, data storage, and archiving you may have

Your AlienVault technical representative can help you analyze your environment to determine system requirements and can provide you with a questionnaire that lists different factors affecting system sizing and scaling, which can help you choose the right system configuration.



Note: The AlienVault [USM Appliance data sheet](#) describes typical event handling performance and capacity benchmarks for a number of different USM Appliance system configurations and options.

Installation, Setup, and Configuration

USM Appliance is relatively simple to install and configure. To enable fast deployment in your specific environment, the USM Appliance All-in-One includes a Getting Started Wizard to guide you through some of the initial set-up tasks. In virtual environments, USM Appliance is packaged as a virtual machine that can be easily installed and configured using virtual resources, such as those managed by VMware ESX or Hyper-V. See [Minimum Virtual Machine Requirements](#) for more details.

Some of the high level steps in performing USM Appliance configuration include

- Install USM Appliance in network topology (DHCP or manual selection of IP addresses of USM Appliance components)
- Open firewall ports for USM Appliance components, if required. See [Firewall Permissions](#) for details.
- Set up local or remote (IPMI or HPE iLO) USM Appliance management
- Change the root password,
- Register USM Appliance
- Synchronize time zone and NTP server
- Configure USM Appliance Sensor, if using
- Configure USM Appliance Logger, if using
- Connect to corporate mail server for email notifications
- Set up additional configuration options, such as high availability, VPN, and plug-in installation and customization

You can use the AlienVault Setup menu to perform most of these tasks. Information on performing these tasks is provided in the [USM Appliance Initial Setup](#) section.

USM Appliance Deployment Types

This section introduces the various USM Appliance components and explains the different deployment types.

USM Appliance Components

All USM Appliance products include these three core components available as hardware or virtual machines. USM Appliance All-in-One combines the Server, Sensor, and Logger components onto a single system.

USM Appliance Sensor

The USM Appliance Sensor is deployed throughout the network to collect logs and monitor network traffic. It provides the five essential USM Appliance security capabilities – Behavioral Monitoring, SIEM, Intrusion Detection, Asset Discovery, and Vulnerability Assessment – for complete visibility.

There must be at least one USM Appliance Sensor. Depending on your corporate requirements, more may be desirable. This is particularly true if you have distributed branches on subnets subordinate to the network at your headquarters.

USM Appliance Server

Aggregates and correlates information that the Sensors gather. Provides single-pane-of-glass management, reporting, and administration.

There is usually just one USM Appliance Server.

USM Appliance Logger

Securely archives raw event log data for forensic research and compliance mandates.

There is usually just one USM Appliance Logger. However, under some circumstances, two may be used. For information, contact [AlienVault Technical Support](#).

USM Appliance Deployment Types

You deploy AlienVault USM Appliance in one of two ways, simple or complex.

Simple Deployment

Deploys all AlienVault USM Appliance components — Sensor, Server, and Logger — in a single machine called USM Appliance All-in-One.

This deployment model has most applicability for smaller environments, for testing, and for demonstrations.

Complex/Distributed Deployment

This model deploys each AlienVault USM Appliance component — Sensor, Server, and Logger — as an individual virtual or hardware machine to create a distributed topology.

This deployment model comes in two versions that increase scalability and performance by provisioning dedicated systems for each component.

USM Appliance Standard

Consists of the following

- USM Appliance Standard Server
- USM Appliance Standard Sensor
- USM Appliance Standard Logger

USM Appliance Enterprise

Consists of the following

- USM Appliance Enterprise Server — includes the Enterprise Server and Enterprise Database
- USM Appliance Enterprise Sensor
- USM Appliance Enterprise Logger



Note: The USM Appliance Enterprise solution is not available as a virtual machine.

AlienVault USM Appliance deployment solutions

	USM Appliance All-in-One	USM Appliance Standard	USM Appliance Enterprise
User Type	Small organizations	Mid-size organizations	Large organizations
Environment	Single-tier deployment	Multi-tier deployments & distributed environment	Multi-tier deployments and distributed environment
Virtual Appliance	x	x	
Hardware Appliance	x	x	x

For more details, see the [USM Appliance data sheet](#).

USM Appliance Deployment Examples

This topic provides topology examples for the three USM Appliance deployment options

- Simple deployment with USM Appliance All-in-One
- Extended simple deployment with a combination of All-in-One and one or more Remote Sensors
- Complex deployment for larger corporations with multiple branches

Example I: Simple Deployment

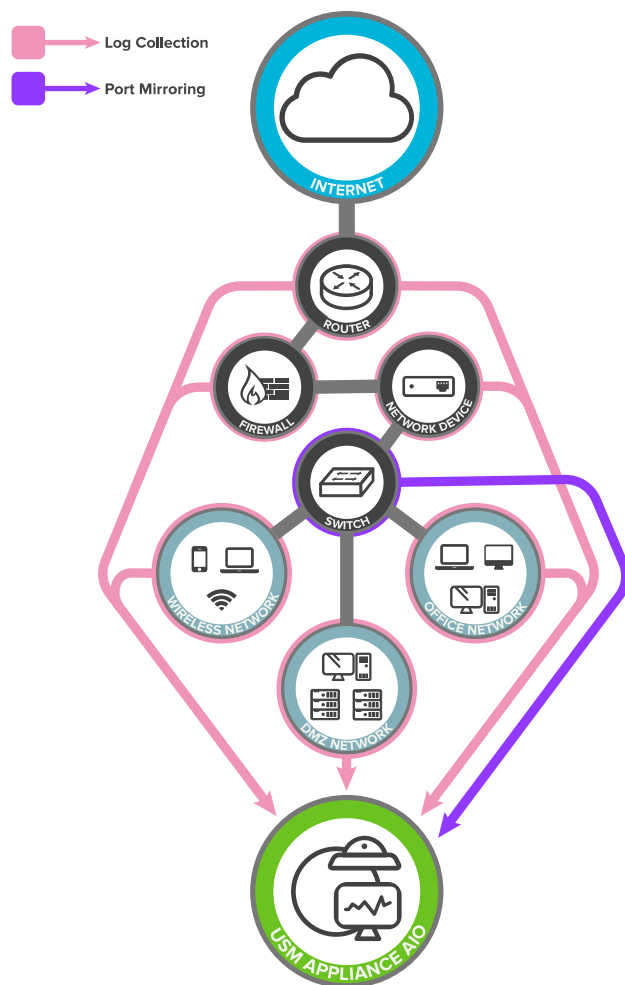
In this example, a USM Appliance All-in-One virtual or hardware appliance is deployed behind the corporate firewall.

The USM Appliance Sensor component on the USM Appliance All-in-One collects logs from the following networks:

- Office network
- Wireless network
- DMZ
- Firewalls

The USM Appliance All-in-One also monitors the network traffic through the connected switches.

These switches must have port mirroring enabled.

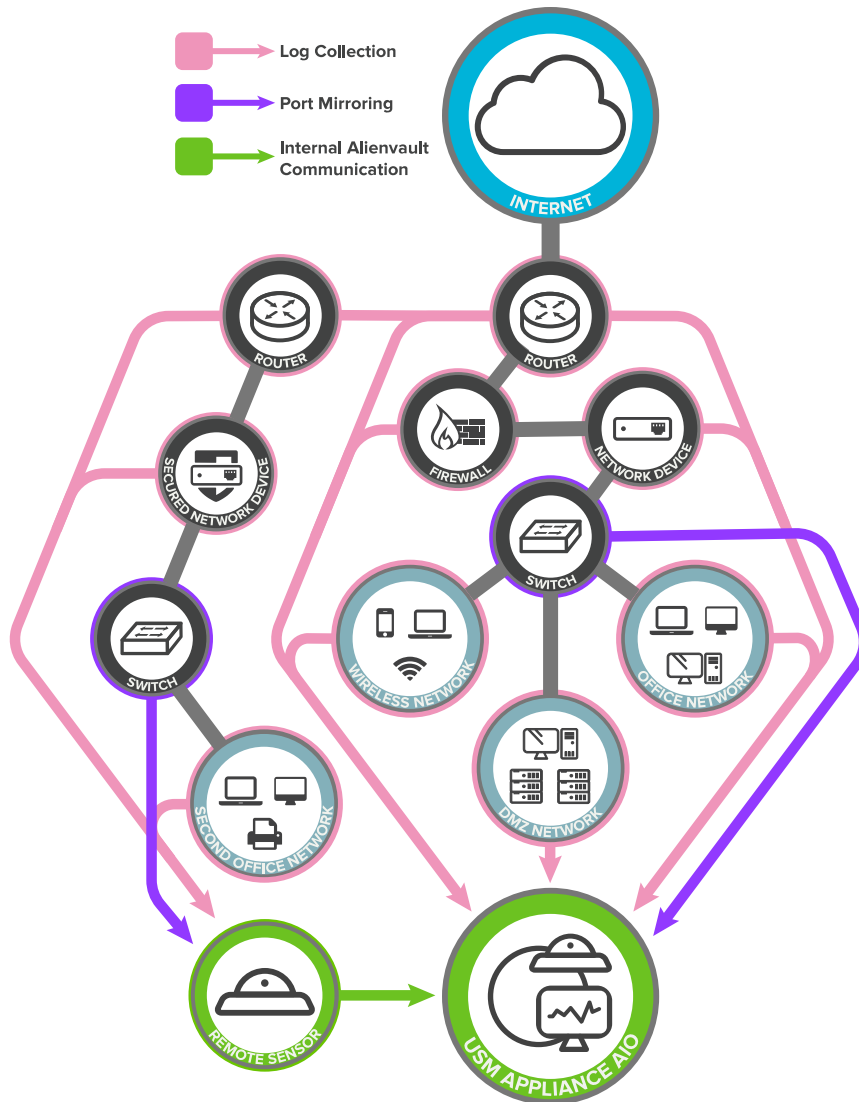


Simple deployment example: USM Appliance All-in-One

Example II: Extended Simple Deployment

This model differs from the Simple Deployment example in that it uses a USM Appliance Remote Sensor for monitoring at a remote office that operates on a subnet. USM Appliance All-in-One is deployed on the main network.

USM Appliance Remote Sensor collects logs and monitors traffic specific to the subnet. It then sends these data to USM Appliance All-in-One on the main network for correlation and risk assessment.



Extended simple deployment example: USM Appliance All-in-One and a remote sensor

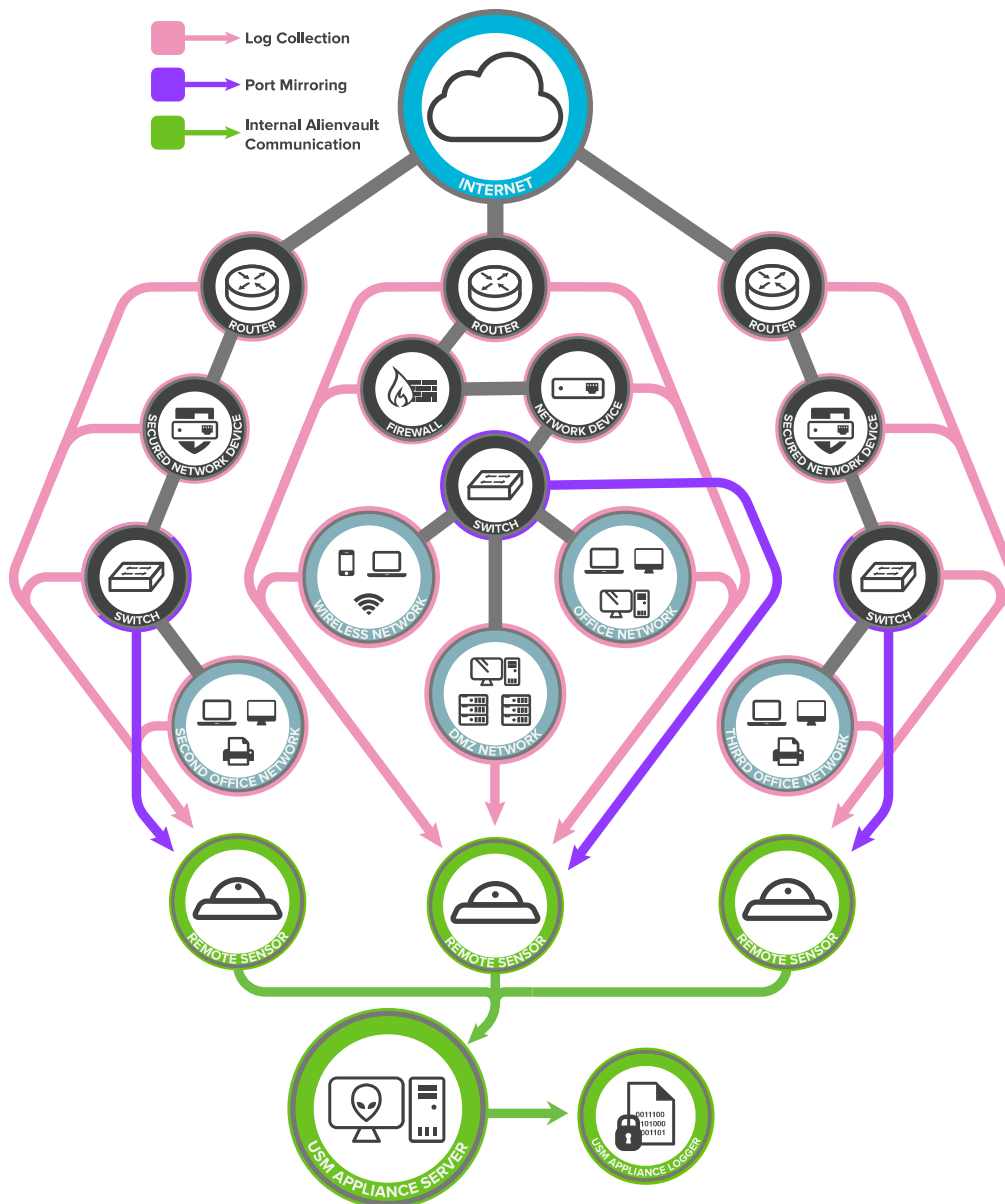
Example III: Complex Deployment

In this deployment example, each office subnet has a remote sensor deployed to collect logs and monitor traffic.

On the main network at headquarters, a single USM Appliance Server, a Logger, and at least one Sensor install as individual appliances to increase scalability and performance.

All USM Appliance Sensors connect to one USM Appliance Server where correlation and risk assessment occur.

The USM Appliance Server forwards the events and alarms to the USM Appliance Logger for long-term storage.




Complex deployment example: individual USM Appliance components

USM Appliance Deployment Requirements

USM Appliance has the following general deployment requirements.

Minimum Hardware Requirements for Virtual Machines

All AlienVault USM Appliance hardware meets the requirement listed in the table below. To achieve sufficient performance, you need to use similar or better hardware to host every AlienVault USM Appliance virtual machine. Hosting USM Appliance virtual machines on inadequate system resources may affect their ability to perform necessary tasks, and also may affect the stated throughput. In addition, if you satisfy the hardware specification but try to run multiple USM Appliance virtual machines on it, the performance degrades.


 **Warning:** In USM Appliance version 5.4, AlienVault updated its Network IDS to include the [Hyperscan library](#), which requires the CPU to support [SSSE3](#) (Supplemental Streaming SIMD Extensions 3) instruction set. To check if your CPU contains SSSE3, see [our knowledge base article](#).

USM Appliance Minimum Required Hardware Specifications

Name	Value
CPU Type	Intel® Xeon E5620
RAM Type	DDR3 1333 MHz
Disk Type	SAS 10000 RPM (204 MB/s)
Memory Performance (MEMCPY)	3310.32 MiB/s
Disk Performance (random read/write)	15.97 MB/s (120 Mb/s)

Minimum Virtual Machine Requirements

The following table lists the minimum system requirements for deploying USM Appliance virtual machines. For a more complete list, see the [USM Appliance data sheet](#) on the AT&T Cybersecurity website.

 **Important:** The virtual machines must operate in Hardware Virtualization Mode (HVM). Paravirtualization is not supported at this time as the device requires SCSI device Bus (SDx) connectors.

USM Appliance Minimum Virtual Machine Requirements

	USM Appliance All-in-One		Remote Sensor		USM Appliance Standard		
	1TB	500GB	1TB	250GB	Server	Logger	Sensor
Total Cores ¹	8		4		8		
RAM (GB) ²	16		8		24		
Storage (TB)	1.0	0.5	1.0	0.25	1.2	1.8	1.2
Virtualization Environment	VMware virtual hardware version 10+ (ESXi 5.5 and later) ³ Hyper-V 3.0+ (Windows Server 2008 SP2 and later)						

¹Total Cores are available physical cores without hyperthreading enabled.

²To guarantee stable operation, you should increase the RAM if the swap space on the hard disk exceeds 1 GB for extended amount of time. Otherwise data collection and normalization, OTX integration, or vulnerability scanning might fail.

³To deploy USM Appliance version 5.7.3 or later, you must be running ESXi 5.5 or later. Previous version of USM Appliance can be deployed on ESXi 4.0 or later.

⁴Due to the way that OTX™ is managed, otx.alienvault.com does not have a fixed IP address and AT&T Cybersecurity cannot provide the IP range.

⁵The USM Appliance API tries to access www.google.com every five minutes to ensure that the system has an Internet connection.

⁶USM Appliance assumes the component to be offline if no response is received from ping.

⁷ This rule is more granular than the default one in msauth_rules.xml, because it matches the different failure reasons reported by event 4625.

Supported Browsers

AlienVault supports the following browsers. All USM Appliance releases are tested on the most recent version of the browsers and one version prior to the most recent.

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

Firewall Permissions

USM Appliance components must use particular URLs, protocols, and ports to function correctly.



Note: If deploying USM Appliance All-in-One, you only need to open the ports associated with the monitored assets, because All-in-One includes both USM Appliance Server and USM Appliance Sensor, therefore the communication between them becomes internal.

If your company operates in a highly secure environment, you must change some permissions on your firewall(s) for USM Appliance to gain access.

External URLs and port numbers used by USM Appliance features

Server URL	Port Number	AlienVault Features in Use	Applicable Release
data.alienvault.com	80	USM Appliance product and feed update	All
maps-api-ssl.google.com	443	Asset Location	All
maps.googleapis.com			
maps.google.com		Asset Location	All
maps.gstatic.com	80		

External URLs and port numbers used by USM Appliance features (Continued)

Server URL	Port Number	AlienVault Features in Use	Applicable Release
messages.alienvault.com	443	Message Center	All
otx.alienvault.com ⁴	443	Open Threat Exchange®	5.1+
reputation.alienvault.com	443	USM Appliance IP Reputation	All
tractorbeam.alienvault.com	22, 443	Remote Support	All
www.google.com ⁵	80	USM Appliance API	All
cybersecurity.att.com/product/help/ping.php ⁶	443	Detects if the USM Appliance component is online	All

¹Total Cores are available physical cores without hyperthreading enabled.

²To guarantee stable operation, you should increase the RAM if the swap space on the hard disk exceeds 1 GB for extended amount of time. Otherwise data collection and normalization, OTX integration, or vulnerability scanning might fail.

³To deploy USM Appliance version 5.7.3 or later, you must be running ESXi 5.5 or later. Previous version of USM Appliance can be deployed on ESXi 4.0 or later.

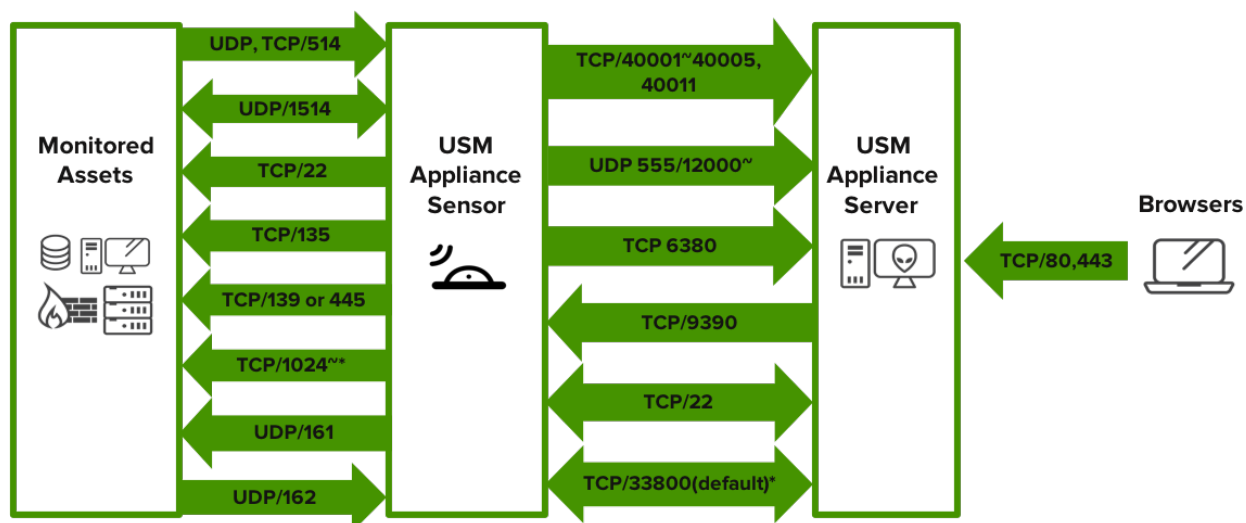
⁴Due to the way that OTX™ is managed, otx.alienvault.com does not have a fixed IP address and AT&T Cybersecurity cannot provide the IP range.

⁵The USM Appliance API tries to access www.google.com every five minutes to ensure that the system has an Internet connection.

⁶USM Appliance assumes the component to be offline if no response is received from ping.

⁷ This rule is more granular than the default one in msauth_rules.xml, because it matches the different failure reasons reported by event 4625.

The following diagram shows the port numbers used by the USM Appliance components to communicate with each other and with the monitored assets. The direction of the arrows indicate the direction of the network traffic.



Port numbers used between USM Appliance components



Important: Ports labeled with * are optional.

- On the hosts you plan to deploy the AlienVault HIDS agents, to allow for initial deployment, you must open TCP port 135, either TCP port 139 or TCP port 445, and high TCP ports (1024 or above). See [Microsoft's documentation on port requirements for Distributed File System Namespaces \(DFS\)](#).
- You also need to open UDP port 1514 for ongoing communication between the AlienVault HIDS agent and the USM Appliance Sensor. For assistance on deployment, see [Deploy AlienVault HIDS Agents](#).
- To use SNMP in USM Appliance, you need to open UDP port 161 on the SNMP agent and UDP port 162 on the USM Appliance Sensor. For more details, see [SNMP Configuration in USM Appliance](#).
- If running USM Appliance versions prior to 5.6.5, you also need to open TCP port 9391 on the Sensor for the vulnerability scanner. But starting from version 5.6.5, vulnerability scans are conducted using the UNIX domain sockets, so port 9391 is no longer used.

About the Use of VPN

Port 33800 shown in the diagram is a default and only used when VPN is enabled. You may use a different port for VPN, if desired.



Note: When enabling the VPN, you do not need to open the other ports between the USM Appliance Sensor and the USM Appliance Server, because all communication goes through the VPN tunnel.

If you enable VPN, in addition to having port 33800/TCP open for the VPN tunnel, you also need to allow TLS transport for that port in case you use a firewall/security device that can perform inspection or interception of TLS traffic.

Configure the USM Appliance Hardware

You can manage the USM Appliance hardware either locally or remotely, through the IPMI or HPE iLO interface. Enabling remote management adds the ability to access the appliance if the operation system is not responsive or does not allow access from the network.

Configure the USM Appliance Hardware Locally

To manage the USM Appliance hardware locally, you must connect a monitor, mouse, and keyboard to the machine.

Starting from version 5.4, AlienVault ships USM Appliance hardware built on Hewlett Packard Enterprise (HPE) ProLiant Gen9 or Gen10 Servers. All prior versions of USM Appliance hardware are built on Supermicro servers. For detailed hardware specifications, see the [USM Appliance data sheet](#) on the AlienVault website.

To connect to the USM Appliance hardware locally

1. Make sure that the appliance is powered off.

The power switch is located on the opposite side of the appliance from the cable ports.

2. On the rear of the appliance, connect the monitor cable to the VGA port, as applicable.
 - Rear view of USM Appliance on Supermicro servers



- Rear view of USM Appliance on HPE ProLiant DL120 Gen9 Servers



- Rear view of USM Appliance on HPE ProLiant DL360 Gen10 Servers with 1Gb interfaces



- Rear view of USM Appliance on HPE ProLiant DL360 Gen10 Servers with 10Gb interfaces



3. Connect the keyboard and mouse.
4. Connect one end of an Ethernet cable to the eth0 port, which is reserved for Administrative setup, and the other to the network switch.
5. Cable the two power cables to each of the power ports on the left-rear side of the appliance and plug the other ends into a power strip.
6. Power on the appliance and turn on the monitor.

The monitor displays the USM Appliance login screen. See [USM Appliance Initial Setup](#) for details.

Configure the USM Appliance Hardware through IPMI

Some USM Appliance hardware is built on Supermicro with IPMI utilities. IPMI (Intelligence Platform Management Interface) enables the monitoring and controlling of servers from remote locations. In this section, we cover the following topics:

Before You Start

Before configuring IPMI on USM Appliance hardware, consider the following:

- IPMI on USM Appliance hardware uses IP address 192.168.200.200 by default, and it does NOT failover to a shared LAN port (eth0 or eth1). This effectively makes it inaccessible to anyone who is not on that internal network.

- AlienVault recommends that you deploy IPMI on an isolated network segment or virtual LAN (VLAN). In addition, configure the IPMI port to be dedicated. See [Configuring a VLAN for IPMI Access](#).
- If the IPMI port must be accessed outside of the network security perimeter, set up a VPN server to provide that access.

For more best practices on managing servers with IPMI features, see [Supermicro's documentation](#).

Configuring USM Appliance (Except Remote Sensor) for IPMI

Follow these steps to configure IPMI on each USM Appliance hardware installation *except* the Remote Sensor, which is on a different IPMI firmware version. You should have connected a monitor and a keyboard to USM Appliance and an Ethernet cable to the IPMI port on the rear of the machine.

For IPMI configuration on the Remote Sensor, see [Configuring USM Appliance Remote Sensor for IPMI](#).

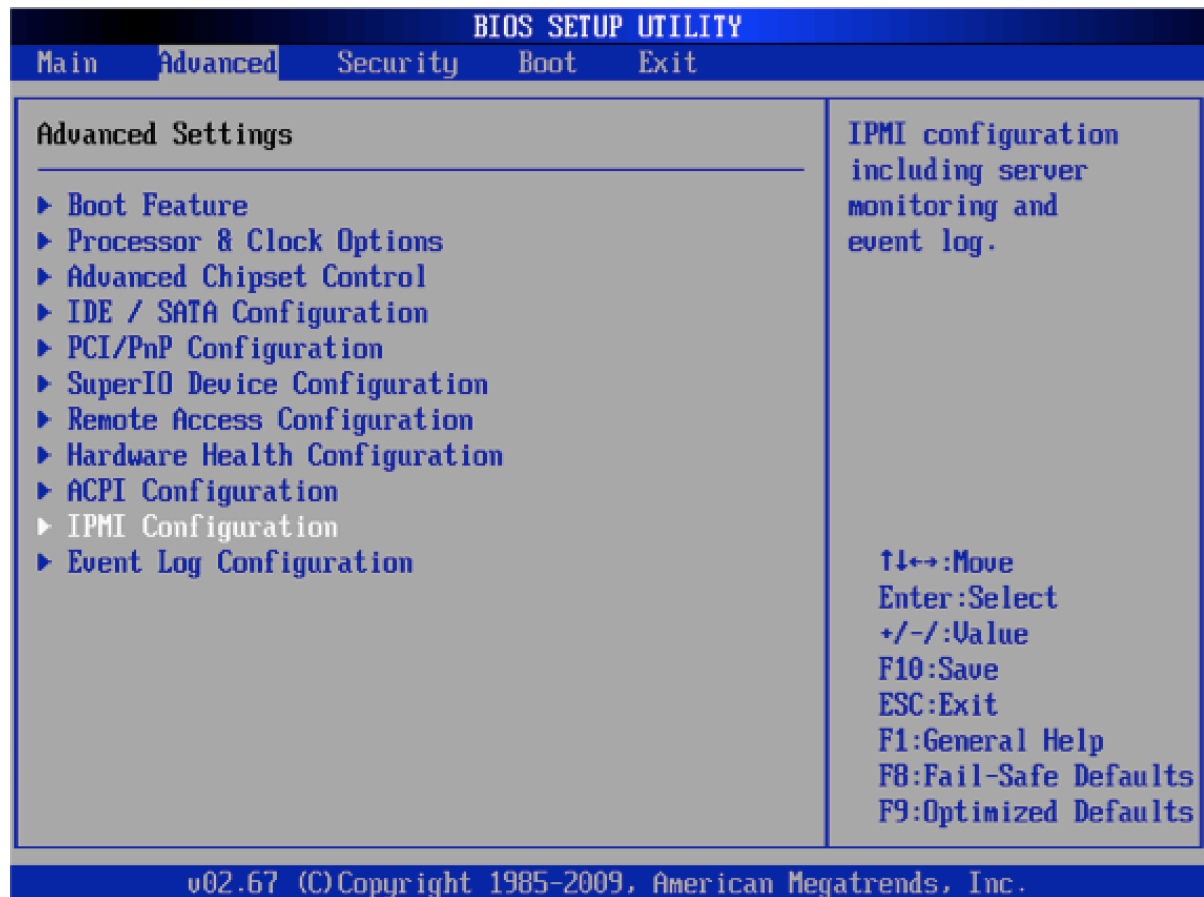
To configure IPMI on the USM Appliance hardware

1. Power on USM Appliance.
2. During startup, press and continuously hold **Delete** on the keyboard.

The BIOS SETUP UTILITY screen appears on the monitor.

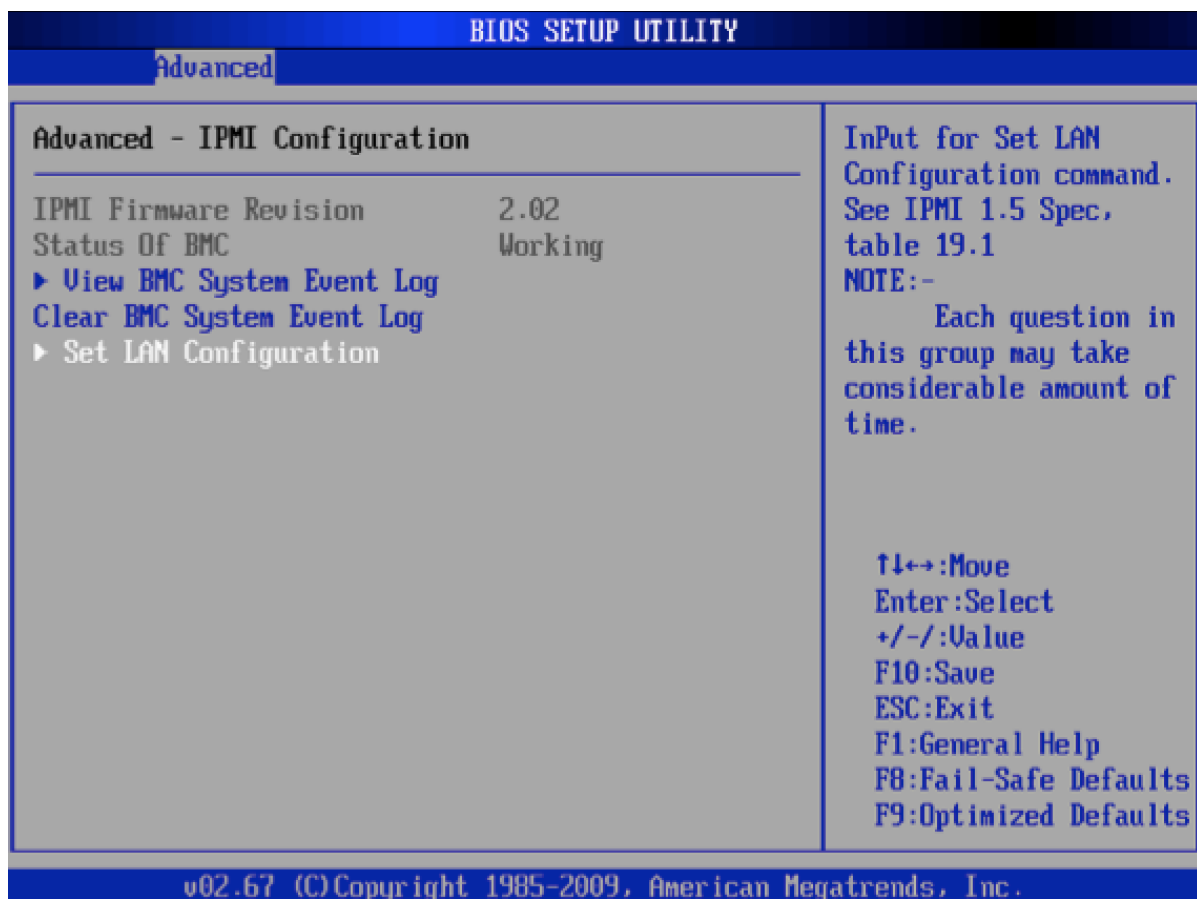
3. Use Tab or the Up/Down and Right/Left Arrow keys to navigate to the **Advanced** tab.

The Advanced Settings panel appears.



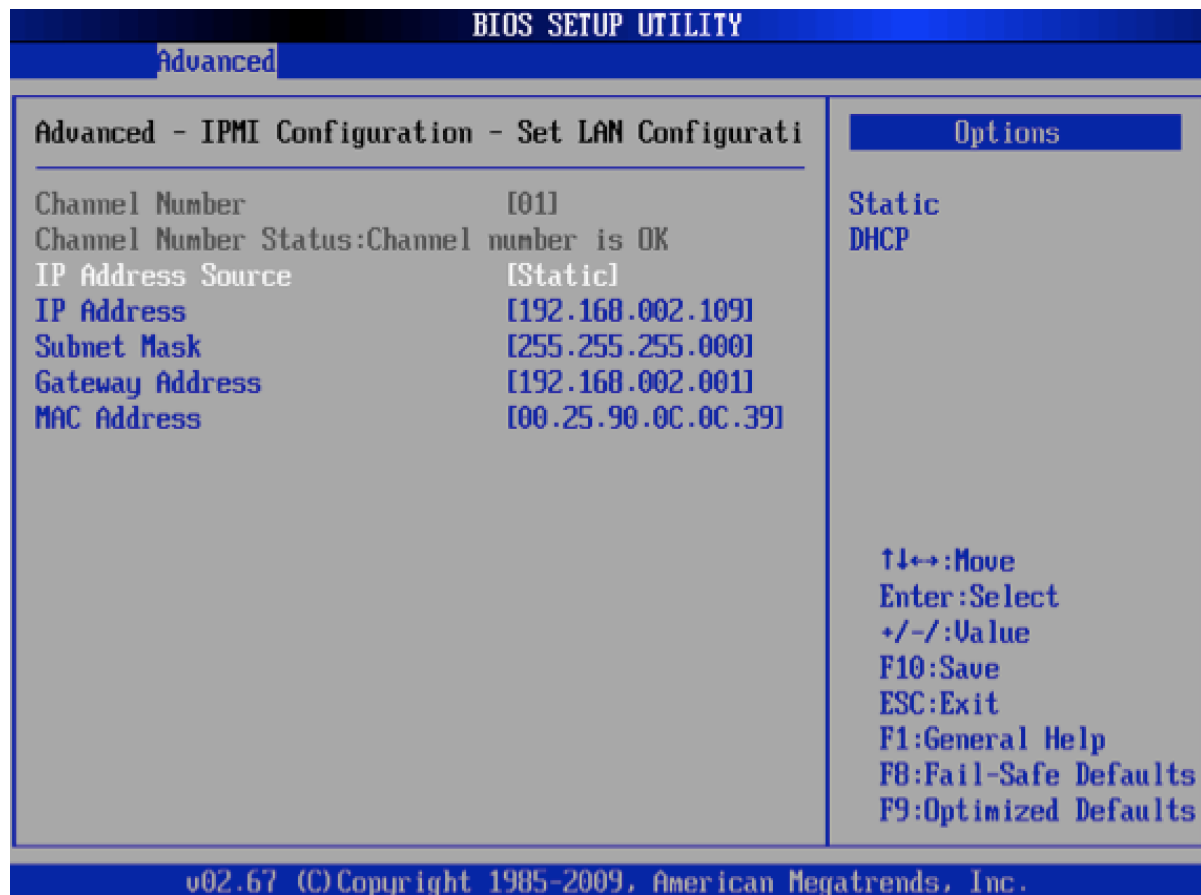
4. Choose **IPMI Configuration** and press **Enter**.

The Advanced - IPMI Configuration panel appears.



5. Choose **Set LAN Configuration** and press **Enter**.

The Advanced - IPMI Configuration - Set LAN Configuration panel appears.



6. Choose a method of assigning an IP address to the machine:
 - If you have a DHCP server in the same network as the USM Appliance hardware, use the Arrow keys to select IP Address Source, and then use plus (+) or minus (-) to change IP Address Source to **DHCP**.
 - If you do not have a DHCP Server, use the arrow keys to select **Static**.
7. (Static IP address users only) Use the Arrow keys to access the IP Address, Subnet Mask, and Gateway Address fields and type the appropriate values in each for your device.



Note: Each machine comes with a default IP address; you may either use this IP address or configure a new one.

8. Save the changes by pressing **F10**, and then press **ESC** to exit the BIOS SETUP UTILITY.
9. You must restart the machine for your changes to take effect.

Configuring USM Appliance Remote Sensor for IPMI

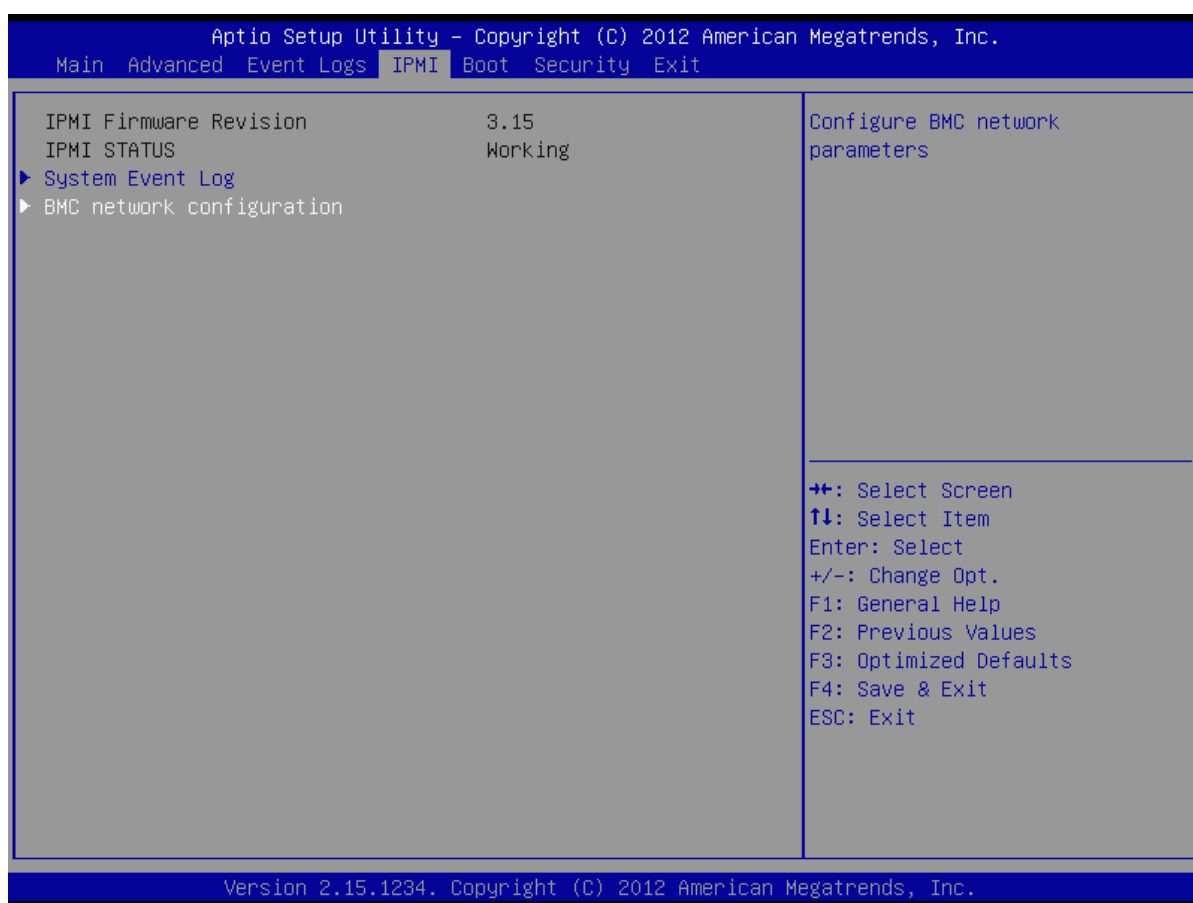
The USM Appliance Remote Sensor requires its own IP address, netmask, and gateway IP addresses.

To configure IPMI on a USM Appliance Remote Sensor

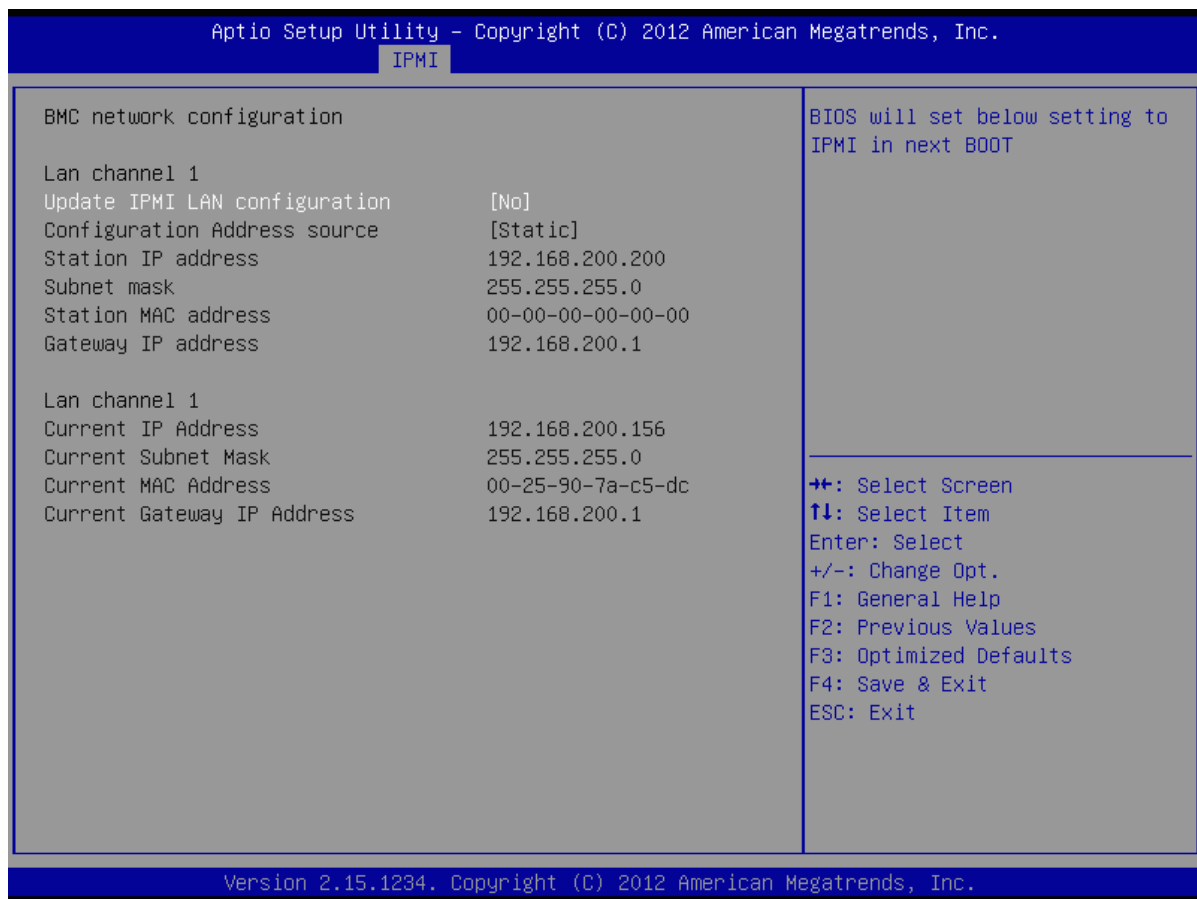
1. Power on the machine.
2. During startup, press and continuously hold **Delete** on the keyboard.

The Aptio Setup Utility appears on the monitor.

3. Using Tab or Arrow, select the **IPMI** tab.



4. Select **BMC network configuration** and press **Enter**.
5. Use Down Arrow to select **Update IPMI LAN configuration** and press **Enter**.



6. Use Tab or Right Arrow to go to the column labeled **[No]**; toggle it to **[Yes]** by using plus (+) or minus (-) and press **Enter**.
7. Choose a method of assigning an IP address to the machine:
 - If you have a DHCP server in the same network as USM Appliance Remote Sensor:
 - a. Use Tab to go to **Configuration IP Address source**, then to **Static** in the right-hand column of that row.
 - b. Toggle Static to DHCP, using plus (+) or minus (-), and press **Enter**.
 - If you do not have a DHCP Server, use Tab or Arrow to go to **Static**; press **Enter**.
8. (Static IP address users only) Use Tab to access the Station IP address, subnet mask, and gateway IP address fields, and type the values applicable to your device in each; press **Enter**.



Note: Each machine comes with a default IP address; you may either use this IP address or configure a new one.

You must restart the machine for your changes to take effect.

Accessing the IPMI Web UI

After you have configured IPMI on USM Appliance, you can connect to USM Appliance through a browser from any computer that is connected to the same network.

To access USM Appliance IPMI through your browser

1. Open a browser on the computer that can access USM Appliance and type the IPMI IP address assigned in the configuration step.

After a connection is made, the Supermicro Login screen appears.

2. Type the default factory username "ADMIN" and password "4L13NV4ULT_0", then click **Login**.

The main IPMI screen appears.

3. After you have successfully logged in, change the default password for security purposes.

You must then log in with the new password.

4. After logging in again, enable display of the remote USM Appliance console and configure redirection:
 - a. On the top menu bar, click **Remote Control**.
 - b. In the navigation pane at left, select **Console Redirection**.
 - c. On the Console Redirection screen, click **Launch Console**.



Note: If the browser blocks it, click the top of the menu bar and select Download File. Then open it from your Downloads folder.

5. When you receive the Java prompt asking whether you want to run the application, click **Run**.



Note: If you receive a warning that the application is untrusted and asking if you want to make an exception, click **Continue**.

Configuring a VLAN for IPMI Access

AlienVault recommends that you deploy IPMI as part of a VLAN.

This procedure describes how to make your VLAN accessible to IPMI.

To configure VPN VLAN IPMI network settings

1. Log into the machine through the browser and enter the IPMI IP address you previously configured.
2. Go to **Configuration > Network**.
3. Within the VLAN section of the page, click **enable**.
4. In the **VLAN ID** field, type a value between 1 and 4095 to identify the VLAN.
5. (Optional) In the LAN interface list, select **Dedicate**.

By selecting Dedicate, you configure IPMI to connect over the IPMI port at all times. Otherwise, it fails over automatically to the two shared LAN ports (eth0 and eth1).

6. Click **Save**.

Updating the IPMI Firmware

AlienVault recommends that you keep the IPMI firmware up-to-date. See the table below for the IPMI firmware versions on USM Appliance. You can download the firmware files directly from [Supermicro Products](#). Search for the motherboard model to locate the files.

IPMI firmware versions on USM Appliance

USM Appliance Hardware	Motherboard Model	IPMI Firmware File
USM Appliance All-in-One	X8DTU-6F+	SMT_326.zip
USM Appliance Standard Server		
USM Appliance Standard Logger		
USM Appliance Standard Sensor 6 x 1GB		
USM Appliance Standard Sensor 2 x 10GB		
USM Appliance Enterprise Server		
USM Appliance Server DB		
USM Appliance Enterprise Logger		
USM Appliance Enterprise Sensor 6 x 1GB		
USM Appliance Enterprise Sensor 2 x 10GB		
USM Appliance Remote Sensor	X9SCL-F	SMT_X9_352.zip
	X10SLH-F	REDFISH_X10_381_unsigned.zip

To update the IPMI firmware

1. Open a browser and type the IPMI IP address of your USM Appliance in the navigation bar.
2. Log in, and then click **Maintenance > Firmware Update**.

The firmware update displays a message about how the update mode affects the device.



System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
<div> <div> Maintenance </div> <div> Firmware Update </div> <div> Unit Reset </div> <div> IKVM Reset </div> <div> Factory Default </div> <div> IPMI Configuration </div> </div> <div> <div> Firmware Update </div> <div> Press Enter Update Mode to put the device in a special mode that allows firmware update. Please note that once you enter update mode the device will reset if the update process is canceled. </div> <div> Enter Update Mode </div> </div>						



Important: After USM Appliance is in the firmware update mode, the update process resets the IPMI device, even if you cancel the update.

- Click **Enter Update Mode** and then **OK**.

The page changes from Firmware Update to Firmware Upload.

- Click **Browse** to choose the firmware file. Make sure that the firmware version is correct before proceeding.



System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
<div> <div> Firmware Upload </div> <div> The device is now in Upgrade mode. Please wait until the percentage of the Firmware Image burning get 100 percent. After that, please just wait for system reboot. The web page will redirect to the Login page automatically. </div> <div> Select Firmware to Upload: Browse... SMT_252.bin Upload Firmware Cancel </div> </div>						

- Click **Upload Firmware**.
- Select **Preserve Configuration** on the following page, so that the system does not change your configuration during reboot.

➔ Firmware Upload

Upgradeable Modules

Module Name ▾
IPMI_FW

☒ **Preserve Configuration**(Unchecking this option will restore the factory default setting of BMC.)

Start Upgrade
Cancel

7. Click **Start Upgrade**.

The update process displays a message showing what percentage of the upload has completed.

SUPERMICR●

System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous
--------	---------------	---------------	----------------	---------------	-------------	---------------

➔ Firmware Upload

The device is now in Upgrade mode. Please wait until the percentage of the Firmware Image burning get 100 percent. After that, please just wait for system reboot. The web page will redirect to the Login page automatically.

Upgrade progress : 74%

!

Warning: Do not interrupt the process. After the upgrade completes, the device will automatically reboot, and you will need to log in again.

8. Log in to the system when prompted.
9. Confirm that the firmware has upgraded to the desired version.

10. Click **Configuration > Date and Time** to update the date and time.

For more details on IPMI, see the [IPMI User's Guide](#) on the Supermicro website.

Configure the USM Appliance Hardware through HPE iLO

Starting from version 5.4, AlienVault ships USM Appliance hardware built on Hewlett Packard Enterprise (HPE) ProLiant Gen9 Servers. Integrated Lights-Out (iLO) is a remote server management processor embedded on the system boards of these servers. HPE iLO enables the monitoring and controlling of servers from remote locations. For security concerns, the USM Appliance hardware provided by HPE has iLO disabled by default. You need to enable HPE iLO from the BIOS before you can use it. And should you choose to do it, AlienVault recommends that you restrict access to HPE iLO by configuring a secure virtual LAN (VLAN), and make sure that the VLAN is connected to a secure network.

About HPE iLO Licensing

All USM Appliance hardware provided by HPE includes the HPE iLO 4 standard features with no additional cost or license requirements.

Before You Start

Before configuring HPE iLO on USM Appliance, you must have performed the following:

- Connect an Ethernet cable to USM Appliance through the HPE iLO management port.
- Connect USM Appliance to a power outlet.
- Make sure you can reach USM Appliance over the network from the machine you are on.
- Install the Java version recommended by HPE on your machine. See the vendor website for up-to-date information.
- If not using DHCP, acquire the IP address you want to assign to HPE iLO.

Enabling HPE iLO

The USM Appliance hardware provided by HPE has iLO disabled by default. You need to enable HPE iLO from the BIOS before you can use it.

To enable HPE iLO

1. Power on or restart USM Appliance.
2. Press the **F9** key, when prompted, to enter **System Utilities**.
3. Select **System Configuration** and then **iLO 4 Configuration Utility**.

4. Select **Setting Options** and then change **iLO 4 Functionality** to "Enabled".
5. Press **F10** to save your changes.
6. Restart the server.

Assigning Static IP Address to HPE iLO

The HPE iLO on the USM Appliance hardware is pre-configured to obtain the IP address from a DHCP server. If you want to use a static IP address instead, you have to change the configuration from the system BIOS.

To manually assign an IP address to HPE iLO

1. Power on or restart USM Appliance.
2. Press the **F9** key, when prompted, to enter **System Utilities**.
3. Select **System Configuration** and then **iLO 4 Configuration Utility**.
4. Select **Network Options**:
 - a. Change **DHCP Enable** to "Off".
 - b. Enter **IP Address**, **Subnet Mask**, and **Gateway IP Address** based on your network setting.
5. Press **F10** to save your changes.
6. Restart the server.

Accessing the HPE iLO Web Interface

You can use the HPE iLO web interface to manage iLO.

To access the HPE iLO web interface

1. Open a web browser and type the IP address assigned to HPE iLO.

The IP address is displayed at the top right corner of the console during a system Power-On Self-Test (POST).

2. Enter the user name and password shown on the sticker label of the appliance.

Each USM Appliance appliance includes a sticker label from the manufacturer, where you can see the HPE iLO's default settings, including the serial number, user name, DNS name, and password.

3. Click **Log In**.

For security reasons, AlienVault recommends that you change the password after you have successfully logged in. You can also add, delete, or edit users from the HPE iLO web interface.

Enabling VLAN on HPE iLO

AlienVault recommends that you restrict access to HPE iLO by configuring a VLAN, and make sure that the VLAN is connected to a secure network.

To enable VLAN on HPE iLO

1. Log in to the HPE iLO web UI.
2. Go to **Network > Shared Network Port**.
3. On the General tab, click **Use Shared Network Port** and leave the default selections for NIC and Port unchanged.
4. To use a VLAN, click **Enable VLAN**.



Note: According to the [4 User Guide](#), when the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN.

5. In the VLAN Tag field, type a value between 1 and 4094 to identify the VLAN.

All VLANs must have a VLAN ID, and all network devices that you want to communicate with each other must have the same VLAN tag.

6. Click **Submit**.

Disabling HPE iLO

The USM Appliance hardware provided by HPE has iLO disabled by default. You need to enable HPE iLO from the BIOS before you can use it. Should you decide to disable it later on, you can do so from the BIOS again.

To disable HPE iLO

1. Power on or restart USM Appliance.
2. Press the **F9** key, when prompted, to enter **System Utilities**.
3. Select **System Configuration** and then **iLO 4 Configuration Utility**.
4. Select **Setting Options** and then change **iLO 4 Functionality** to "Disabled".
5. Press **F10** to save your changes.
6. Restart the server.

Updating the HPE iLO Firmware

AlienVault recommends that you keep the HPE iLO firmware up to date. See the table below for the HPE iLO firmware versions on USM Appliance.

HPE iLO firmware versions on USM Appliance

HPE iLO Firmware Version	USM Appliance Hardware
HPE DL 120 Gen9,	USM Appliance All-in-One
HPE DL 360 Gen10	USM Appliance Standard Server
	USM Appliance Standard Logger
	USM Appliance Standard Sensor 6 x 1GB
	USM Appliance Standard Sensor 2 x 10GB
	USM Appliance Enterprise Server
	USM Appliance Server DB
	USM Appliance Enterprise Logger
	USM Appliance Enterprise Sensor 6 x 1GB
	USM Appliance Enterprise Sensor 2 x 10GB
HPE DL 20 Gen9	USM Appliance Remote Sensor

HPE provides different ways to update the iLO firmware, but AlienVault recommends using the HPE iLO web interface method. It contains two main steps:

1. Download the HPE iLO firmware image file. See [Obtaining the iLO firmware image file](#) by the vendor.
2. Update the firmware from the HPE iLO web interface. See [Updating iLO or server firmware by using the iLO web interface](#) by the vendor.

For more details on HPE iLO, see the [HPE iLO 4 User Guide](#) on the Hewlett Packard Enterprise website.

Deploy USM Appliance in VMware

AlienVault offers USM Appliance for VMware in a Open Virtual Appliance (OVA) package, which is a tar archive file with the OVF (Open Virtualization Format) directory inside. You can deploy USM Appliance using VMware vSphere Desktop Client, which this document entails. For instructions specific to a different VMware client, consult the vendor documentation directly.

Prerequisites

Before deploying the USM Appliance virtual machine, make sure you have met the [Minimum Hardware Requirements for Virtual Machines](#) as well as the [Minimum Virtual Machine Requirements](#).

You must also have downloaded the VMware image file from AlienVault and unzip it to a location where you can access from the VMware vSphere Client.

Deploy the VMware Image



Note: The deployment steps are the same for USM Appliance free trials and licensed versions.

To deploy USM Appliance in vSphere Desktop Client

1. Under **File**, select **Deploy OVF Template**.
2. In the Deploy OVF Template screen, browse to the USM Appliance virtual image file; click **Next**.
3. On each of the following screens, click **Next** to keep the default values:
 - OVF Template Details
 - Name and Location
 - Storage
 - Disk Format
 - Network Mapping
4. On the Ready to Complete screen, select **Power on after deployment**, located below the list of deployment settings and click **Finish**.

Deployment of the virtual image requires several minutes. After deployment is finished, VMware displays:

```
Deployment Completed Successfully.
```



Important: If deploying the OVA file fails and you receive the following error:

```
The OVF package is invalid and cannot be deployed.
The following manifest file entry (line 1) is invalid: SHA256
(xxxxxxx.ovf)
```

it is because the vSphere Desktop Client does not support SHA256. (This is not an issue if you use the vSphere Web Client or ESXi Web Client to deploy the image.) To work around the issue, you can use the *OVFTool* from VMware to change SHA256 to SHA1. See [this VMware article](#) for instructions. You will be able to deploy the SHA1 OVA file after the conversion.

5. Click **Close**.
6. Connect to the USM Appliance virtual machine in one of the following ways:
 - On the Inventory screen, click **Virtual Machine** and in its submenu; click **Open Console**.
 - In the console toolbar, click the console icon.

The monitor should now display the initial login screen.



Note: Since USM Appliance Sensors do not have a web UI, you cannot access them through a browser. Follow [Configure the USM Appliance Sensor after Deployment](#) to finish the configuration.

Monitor VMware Standard Virtual Switches

This section provides instructions for VMware Standard Virtual Switches (vSwitches). For help on VMware vSphere Distributed Switches (VDS), see [instructions from VMware](#).

USM Appliance virtual machines have six network interfaces: one for management (eth0) and the other five for log collection and/or traffic capture on the network segment monitored. Connecting the monitoring interface(s) to a SPAN (Switched Port Analyzer) port, sometimes also called a mirror port, provides the following capabilities:

- Network IDS
- NetFlow and traffic monitoring
- Passive asset identification

For USM Appliance to monitor traffic from your physical network, you need to allocate a spare NIC (Network Interface Card) on your VMware server to pass the SPAN port traffic to the virtual network. AlienVault recommends that you SPAN your internal firewall ports, connect the SPAN port to the spare NIC, and then associate the spare NIC with a vSwitch.



Important: USM Appliance provides multiple network interfaces to monitor your network. You should not connect them all to the same vSwitch. Instead, you can connect each interface to a different vSwitch that mirrors a different subnet within your network.



Note: The following procedure is based on the ESXi 6.5 Web Client. If you are using a different client or an earlier version of VMware products, please consult the vendor documentation accordingly.

To monitor network traffic through a vSwitch

1. Direct traffic from your physical network to the virtual network.
 - a. Enable port mirroring on the network you want USM Appliance to monitor.
 - b. Allocate a spare NIC on your VMware server to receive the mirrored traffic.
 - c. Associate your spare NIC with the vSwitch.
2. In the ESXi 6.5 Web Client, click **Networking** in the Navigator and select the **Port groups** tab.



Note: In VMware terminology, a port group acts like a network hub, making the network traffic undergoing the vSwitch visible to all interfaces connected to this port group.

3. Click **Add port group**.

Add port group - VM Test Network

Name	VM Test Network
VLAN ID	4095
Virtual switch	vSwitch1
Security	
Promiscuous mode	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch
MAC address changes	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
Forged transmits	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch

Add Cancel

- a. Enter a name for the port group.
- b. In VLAN ID, select **4095** for the VGT (Virtual Guest Tagging) mode.

See [VLAN Configuration](#) in the VMware documentation for more information about VLAN tagging modes.
- c. In Virtual switch, select the vSwitch associated with the spare NIC configured in Step 1.
- d. Expand the Security section and set Promiscuous mode to **Accept**.

This setting assures any virtual interface connected to this port group will be able to enter promiscuous mode and capture traffic from any other virtual interfaces connected to the vSwitch.

4. Click **Add** to create the port group.
5. Next, you need to edit the USM Appliance node you have deployed and connect one or more interfaces to the port group.

▶ Memory	24576	MB	▼
▶ Hard disk 1	1024	GB	▼
▶ SCSI Controller 0	LSI Logic Parallel ▼		
▶ Network Adapter 1	VM Network ▼		<input checked="" type="checkbox"/> Connect
▶ Network Adapter 2	VM TEST Network ▼		
Status	VM Network		
Adapter Type	E1000 ▼		
MAC Address	Automatic ▼	00:50:56:93:a3:ca	
▶ Network Adapter 3	VM Network ▼		<input checked="" type="checkbox"/> Connect
▶ Network Adapter 4	VM Network ▼		<input checked="" type="checkbox"/> Connect

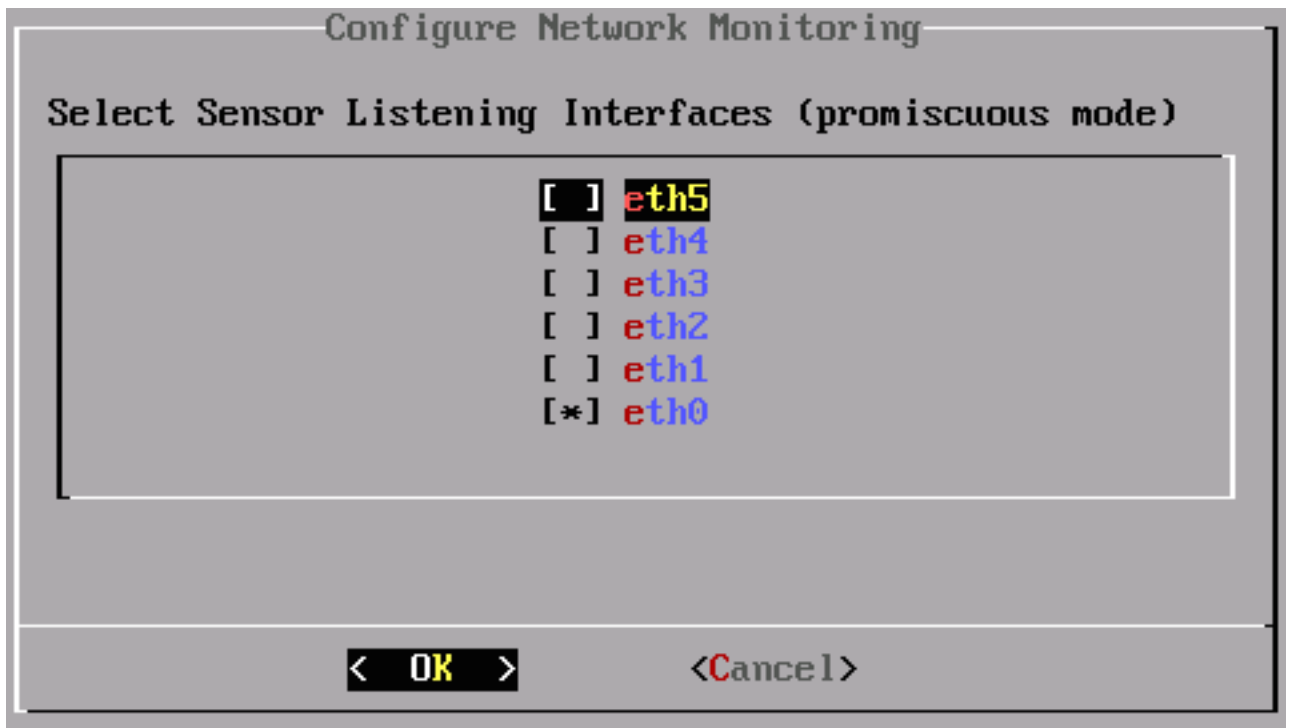
Repeat the steps for every vSwitch you want to monitor.

And lastly, you need to configure network monitoring in the AlienVault Console:

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

The AlienVault Setup menu displays.

2. Select **Configure Sensor**.
3. Select **Configure Network Monitoring**.
4. Use the keyboard arrow keys to move to the interface assigned to the SPAN port group configured previously, select the interface by pressing the spacebar, and then press Enter (<OK>).



5. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
6. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Repeat the steps for every listening interface you want to enable.

Deploy USM Appliance Using Hyper-V Manager

Microsoft Hyper-V is a hypervisor that lets you create and manage virtual machines by using virtualization technology built into Windows Servers. Starting from USM Appliance version 5.3.4, AlienVault offers USM Appliance for Hyper-V in a Virtual Hard Disk (VHD) format, tested on the latest version of the following Windows operating systems

- Windows Server 2008 SP2
- Windows Server 2008 R2 SP2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

You can deploy USM Appliance using Microsoft Hyper-V Manager, an administrative tool for managing local and remote Hyper-V hosts.

Prerequisites

The requirements for deploying USM Appliance in Hyper-V are the same as for the other virtual appliances that AlienVault supports. See [Minimum Virtual Machine Requirements](#) for details. However, to meet the requirements, you must enable hyper-threading from the system BIOS first. Refer to [this virtualization blog post](#) from Microsoft for explanation.

You must also have downloaded the Hyper-V image file from AlienVault and unzip it to a location where you can access from the Hyper-V Manager.



Note: Due to the size of the image file, the built-in zip utility on Windows Server 2008 (all versions) cannot unzip the file. You can use 7-Zip or WinZip instead.

Create the Virtual Machine

To create a virtual machine using the Hyper-V Manager

1. Open the Hyper-V Manager.
2. In the **Actions** panel, click **New > Virtual Machine**.

The **New Virtual Machine Wizard** opens.

3. Go to **Specify Name and Location** and type a name for your new virtual machine

New Virtual Machine Wizard

Specify Name and Location

Before You Begin
Specify Name and Location
 Specify Generation
 Assign Memory
 Configure Networking
 Connect Virtual Hard Disk
 Installation Options
 Summary

Choose a name and location for this virtual machine.


The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name:

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☒ Store the virtual machine in a different location

Location:

 If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

< Previous Next > Finish Cancel

4. Click **Next**.
5. Choose **Generation 1** for this virtual machine and click **Next**.
6. Change the value of the **Startup Memory**
 - For USM Appliance Standard deployment options (including Standard Server, Standard Logger, and Standard Sensor), type **24576 MB**.
 - For USM Appliance All-in-One, type **16384 MB**.
 - For USM Appliance Remote Sensor, type **8192 MB**.
7. Click **Next**.
8. Select the network adapter to the network you want to monitor and click **Next**.
9. Select **Use an existing virtual hard disk** and click **Browse** to locate the Hyper-V VHD file.
10. Click **Next** and on the summary page, click **Finish**.

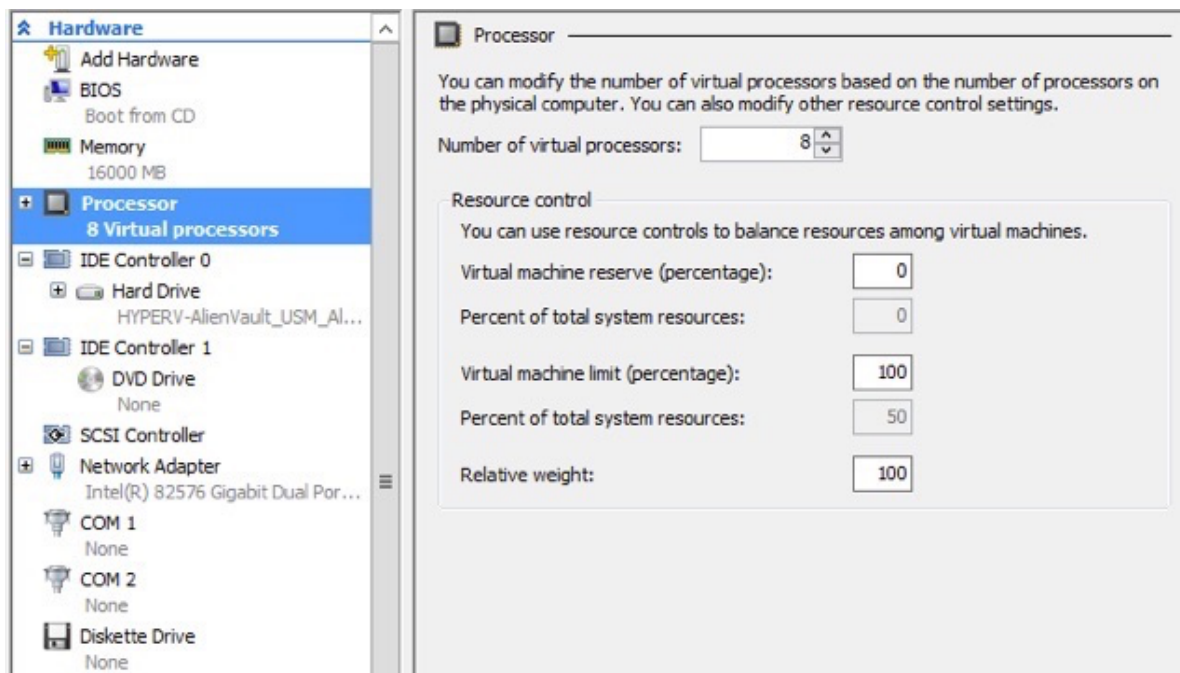
Configure the Virtual Machine

To configure a virtual machine using the Hyper-V Manager

1. Select the USM Appliance virtual machine that you created and click **Settings**.

A new window opens.

2. Click **Processor** in the left panel,
 - For USM Appliance All-in-One and USM Appliance Standard deployment options (including Standard Server, Standard Logger, and Standard Sensor), select **8** number of virtual processors.
 - For USM Appliance Remote Sensor, select **4** number of virtual processors



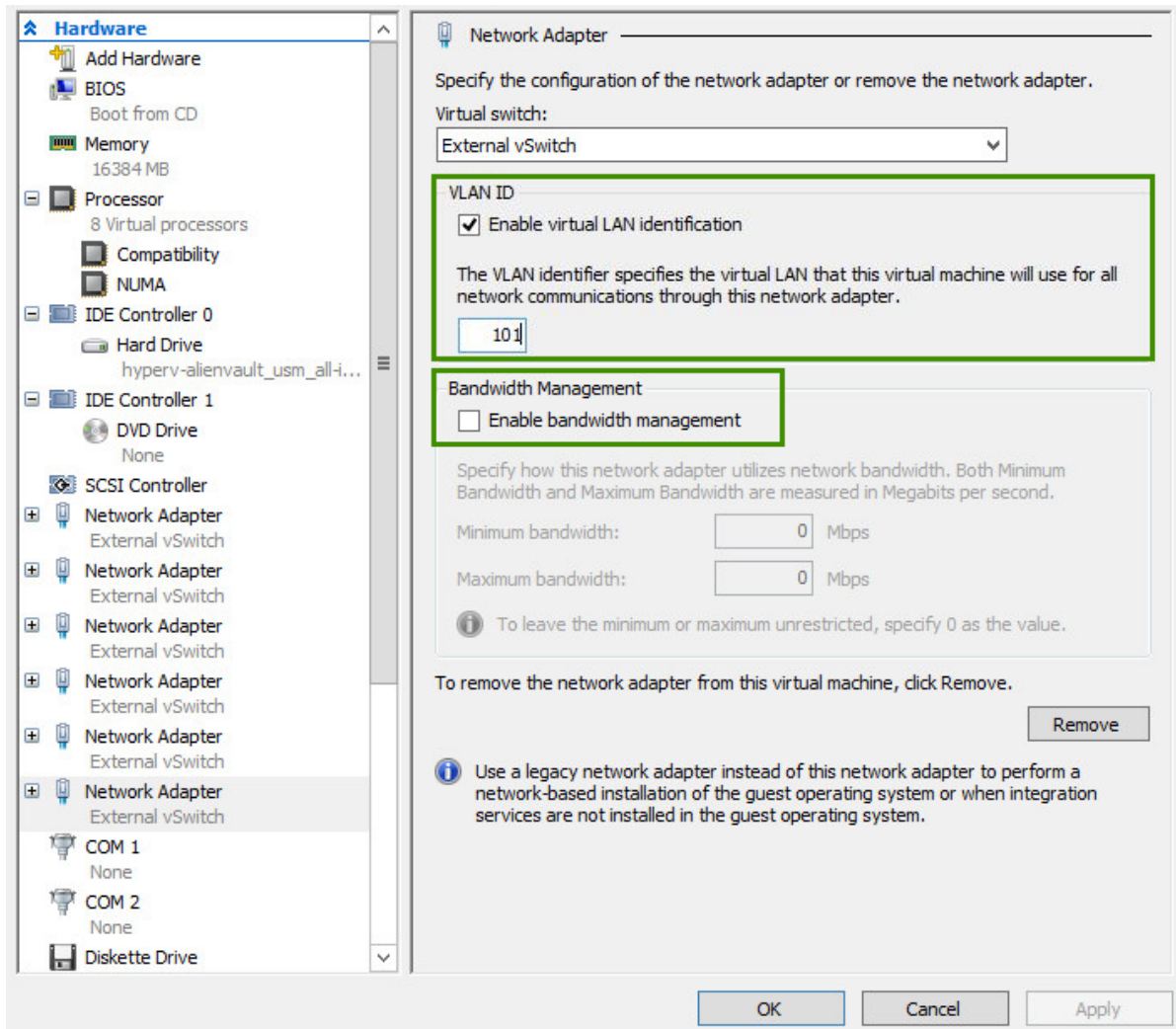
3. Click **Apply**.
4. Click **Add Hardware > Network Adapter > Add** to add network interfaces.



Note: USM Appliance All-in-One supports 6 network interfaces and USM Appliance Remote Sensor supports 2 network interfaces. AlienVault recommends that you have at least two network interfaces, one for management and the other for network IDS.

5. (Optional) If using VLAN, in **VLAN ID**, select **Enable virtual LAN identification** and specify the VLAN ID in the box.

6. In **Bandwidth Management**, leave the option unchecked since enabling bandwidth management introduces the risk of packet loss.



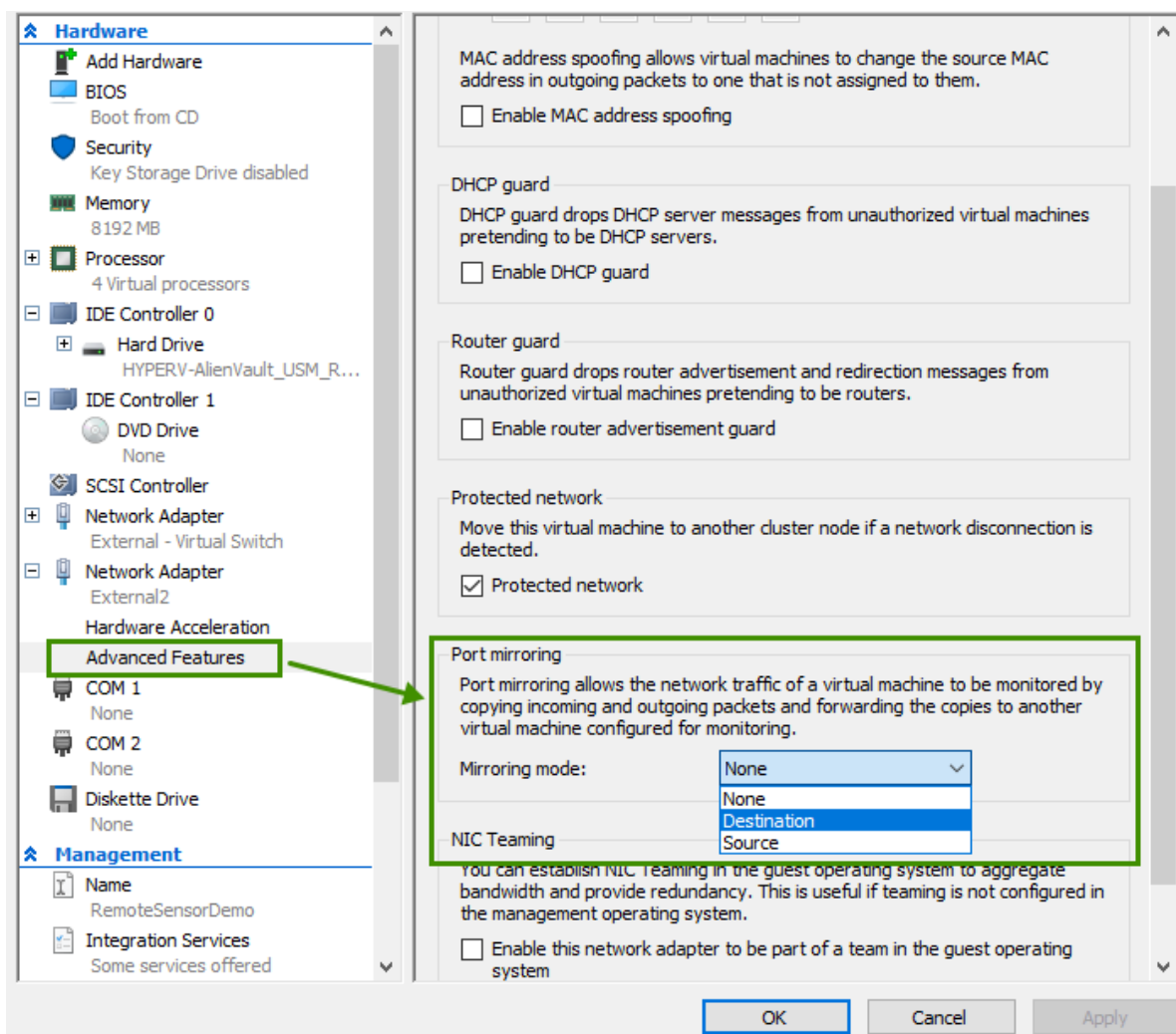
7. Click **Apply**.
8. Repeat Steps 4 through 7 to add more network interfaces.

Configure Port Mirroring

Note: This procedure is optional. Port mirroring configuration is only supported in Windows Server 2012 and later.

To configure port mirroring, follow the steps below when adding network adapters

1. In the left panel, click the plus sign (+) next to the network adapter you are adding, and then click **Advanced Features**.
2. Locate **Mirroring mode** in the Port mirroring section, select **Destination**, and then click **OK**.



3. Open a PowerShell session as administrator.
4. To setup virtual switches in promiscuous mode for monitoring external traffic, run the following:

```
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
$portFeature.SettingData.MonitorMode = 2
Add-VMSystemSwitchExtensionPortFeature -ExternalPort -SwitchName <mySwitch> -VMSystemSwitchExtensionFeature
$portFeature
```

where

<mySwitch> denotes the name of the virtual switch.

With this example, all traffic going through the virtual switch will be mirrored to any VM whose mirroring mode has been set to "Destination".

- Alternatively, to setup virtual switches in promiscuous mode for monitoring internal traffic, run the following:

```
$portFeature=Get-VMSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
$portFeature.SettingData.MonitorMode = 2
Add-VMSwitchExtensionPortFeature -ManagementOS -VMSwitchExtensionFeature $portFeature
```



Note: The -ManagementOS option does not allow you to specify a switch, so *all* virtual switches, including the shared management NIC port, will be set in monitoring mode.

- To setup virtual switches in promiscuous mode for monitoring both internal and external traffic, run the following:

```
$portFeature=Get-VMSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
$portFeature.SettingData.MonitorMode = 2
Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName <mySwitch> -VMSwitchExtensionFeature
$portFeature
Add-VMSwitchExtensionPortFeature -ManagementOS -VMSwitchExtensionFeature $portFeature
```



Note: In the steps above, MonitorMode 0 = None, 1 = Destination, and 2 = Source.

Start the Virtual Machine

To start the virtual machine using the Hyper-V Manager

- Select your virtual machine and click **Start** on the right panel.
- The system initialization screen appears and you will see the console to access USM Appliance from the command line.

Deploy USM Appliance with AMI

In this section, you will learn

- [Deploy the USM Appliance AMI](#)
- [Connect to the AMI Through a Console](#)

Before You Start

After purchasing the USM Appliance AMI, you must send your Amazon identifier and the region you want the AMI deployed to AlienVault Support, who will use that information to share the private USM Appliance AMI with you.

Supported AWS regions:

- ap-northeast-1
- ap-northeast-2
- ap-south-1
- ap-southeast-1
- ap-southeast-2
- eu-central-1
- eu-west-1
- eu-west-2
- us-east-1
- us-west-1
- us-west-2

Deploy the USM Appliance AMI

To deploy the AlienVault USM Appliance AMI

1. Sign in to your Amazon portal.
2. Click **EC2**.
3. Click **Launch Instance**.
4. Click **My AMIs** (on the navigation tree located on the left).
5. In the search field, enter "AlienVault_USM" and click **Select**.
6. Choose an **Instance Type** based on the following recommendation:

Recommended Instance Type for the USM Appliance AMI

Image Name	Recommended Instance Type
USM Appliance All-in-One	m4.2xlarge (8 cores/30GB) or c3.4xlarge (16 cores/30GB)
USM Appliance All-in-One Lite	m4.2xlarge (8 cores/30GB) or c3.4xlarge (16 cores/30GB)
USM Appliance Federation Server	m4.2xlarge (8 cores/30GB) or c3.4xlarge (16 cores/30GB)
USM Appliance Remote Sensor	m4.xlarge (4 cores/15GB)
USM Appliance Remote Sensor Lite	m4.xlarge (4 cores/15GB)
USM Appliance Standard Logger	m4.2xlarge (8 cores/30GB) or c3.4xlarge (16 cores/30GB)
USM Appliance Standard Server	m4.2xlarge (8 cores/30GB) or c3.4xlarge (16 cores/30GB)
USM Appliance Standard Sensor	m4.2xlarge (8 cores/30GB) or c3.4xlarge (16 cores/30GB)

7. Click the square to the left of an instance, and then click **Next: Configure Instance Details**.
8. Select **Launch as EBS-optimized instance** to improve the disk performance.
9. Click **Next: Add Storage**.
10. Click **Volume Type** and choose "Provisioned IOPS". For optimal performance, set the **IOPS** value to "20000". See [Amazon documentation](#) for more details.
11. Click **Next: Tag Instance**.
12. In the **Value** field, type a name for your appliance, and then click **Next: Configure Security Group**.
13. Click **Add Rule** to add `HTTPS`. This protocol allows Internet traffic to reach your USM Appliance instance.



Note: You do not need to add this rule if you are configuring a USM Appliance Sensor, which does not have a web interface.

14. (Optional) Click **Add Rule** to add `HTTP`. This protocol allows web traffic redirection to work in your USM Appliance instance.



Note: You do not need to add this rule if you are configuring a USM Appliance Sensor, which does not have a web interface.

15. Click **Review and Launch**.
16. Review your configuration and click **Launch**.

17. Select **Proceed without a key pair** and **I acknowledge that I have...**
18. Click **Launch Instances**.
19. Click the instance launched.

The instance can have the following status checks:

Initializing. The image has not yet been deployed by Amazon.

1/2 checks. The image has been deployed, but it is not accessible. The image is still configuring.

2/2 checks. The image is ready and completely configured.



Note: Wait a few minutes before trying to log in for the first time. The database may need more time to finish initializing. If you try to log in before, you may see a Database Connection error in the browser.

Connect to the AMI Through a Console

To access the AMI through a console

1. Open a terminal and enter the following command:

```
SSH root@<publicDNS>
```

where

<publicDNS> refers to the default DNS assigned to AlienVault USM Appliance.

2. Login to the system.

The default credential is `root/alienvault`.

3. After logging in for the first time, the system will request a password change.

Configure the USM Appliance Sensor after Deployment

You'll want to set up and configure the USM Appliance Server first. If you purchased USM Appliance Standard, Enterprise, or Remote Sensors, next you will want to configure the sensor by providing the USM Appliance Server IP address and Framework IP address through the AlienVault Setup menu. Then, there are some final configuration steps on the web UI.

Prerequisites

- **USM Appliance All-in-One** — You must have already configured the USM Appliance All-in-One before you can complete the sensor configuration.
- **USM Appliance Standard or Enterprise** — You must have already configured the USM Appliance Server and have its IP address available.
- If you intend to configure VPN in your USM Appliance deployment, you must set up a VPN tunnel for the client beforehand. This provides you with a VPN IP address that you use in this configuration task. For details, see [VPN Configuration](#).

Configure the USM Appliance Sensor

To configure a sensor on USM Appliance All-in-One or USM Appliance Server

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

The AlienVault Setup menu displays.

2. Select **Configure Sensor**.
3. Select **Configure AlienVault Server IP**.
4. Type the IP address of the USM Appliance Server the sensor should contact and press Enter (<OK>).



Important: If this USM Appliance deployment will use VPN, substitute the **VPN IP** for the physical IP address.

The Configure Sensor menu appears again.

5. Select **Configure AlienVault Framework IP**.
6. Type the same IP address you did for the server and press Enter (<OK>).
- The application returns you to the Configure Sensor menu.
7. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
8. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

9. Launch the USM Appliance web UI and log in as administrator.
10. Go to **Configuration > Deployment > Components > Sensors**.

A warning message appears, stating:

The following sensors are being reported as enabled by the server, but are not configured.

The warning message contains the sensor IP address and two links labeled *Insert* and *Discard*.

11. Click **Insert**.

A new screen containing a form appears. To answer the monitor network question, see About Correlation Contexts for assistance.

12. Fill out the form and click **Save**.

13. Repeat all of the foregoing procedures for every sensor you plan to deploy in your network.

Configure the USM Appliance Logger after Deployment

You will need to configure the USM Appliance Logger if you are deploying one of the following:

- USM Appliance Standard or Enterprise solution
- Using USM Appliance All-in-One, but deploying one or more *additional* USM Appliance Loggers to the one that comes with the All-in-One

Unlike the Standard/Enterprise USM Appliance Server and Sensors, the USM Appliance Logger can only be configured through the USM Appliance web UI.



Note: If you want to configure high availability in a USM Appliance Standard or Enterprise deployment, do not complete this logger configuration task until **after** you have completed HA configuration of your two USM Appliance Logger nodes. See [Configuring High Availability for USM Appliance Standard Loggers](#).

Prerequisites

- You must have already deployed the USM Appliance Server and USM Appliance Logger, and completed the initial setup tasks.
- If using USM Appliance version 5.5.1 or later, you must set a remote key on the USM Appliance Server for the USM Appliance Logger to authenticate the system. To set the key, go to


Configuration > Administration > Main > Login Methods/Options > Remote login key.

While there is no constraint on the key, AlienVault recommends that you use something difficult to break, such as a GUID (Globally Unique Identifier).

- If you intend to configure VPN in your USM Appliance deployment, you must set up the VPN tunnel beforehand. This provides you with a VPN IP address that you use in this configuration task. For details, see [VPN Configuration](#).
- If you do not plan to use a VPN, be aware that USM Appliance Logger receives events through TCP/40001. Make sure traffic can go through that port on your network.

Add USM Appliance Server to USM Appliance Logger

After deploying the USM Appliance Logger and finishing the initial setup tasks, you need to establish the connection between the USM Appliance Logger and the USM Appliance Server or the USM Appliance All-in-One.

 **Important:** Because the USM Appliance Server forwards events to the USM Appliance Logger, the logger is considered the parent server. For this reason, you must add the USM Appliance Server as a child to the USM Appliance Logger, and then configure event forwarding on the USM Appliance Server.

To add the USM Appliance Server to the USM Appliance Logger

1. Log into the USM Appliance Logger web UI.
2. Go to **Configuration > Deployment > Servers** and click **Add Server**.

DEPLOYMENT

COMPONENTS	PLUGIN BUILDER	LOCATIONS
------------	----------------	-----------


ALIENVAULT CENTER	SENSORS	SERVICES	REMOTE INTERFACES
-------------------	---------	----------	-------------------

SHOW 20 ENTRIES

CONNECT TO USM CENTRAL **ADD SERVER** DELETE SELECTED MODIFY <>

IP	NAME	PORT	SIEM	RISK ASSESSMENT	CORRELATION	CROSS CORRELATION	SQL STORAGE	ALARM SYSLOG	IP REP	LOGGER	SIGN	FORWARD ALARMS	FORWARD EVENTS
	VirtualUSMStandardLogger	40001	✓	✓	✓	✓	✓	✓	✓	✓	Block	✓	✓

3. Type the IP address and root password of the USM Appliance Server; click **Save**.

 **Important:** If this USM Appliance deployment uses VPN, substitute the **VPN IP** for the physical IP address.

4. Return to the Servers screen, and select the USM Appliance Logger; click **Modify**.

- On the next page, click No for all the options on the form **except Log**; click Yes there.
- Click **Save**.

DEPLOYMENT

COMPONENTS

PLUGIN BUILDER

LOCATIONS

ALIENVault CENTER

SENSORS

SERVERS

REMOTE INTERFACES

SHOW 20 ENTRIES

CONNECT TO USM CENTRAL

ADD SERVER

DELETE SELECTED

MODIFY

IP	NAME	PORT	SIEM	RISK ASSESSMENT	CORRELATION	CROSS CORRELATION	SQL STORAGE	ALARM SYSLOG	IP REP	LOGGER	SIGN	FORWARD ALARMS	FORWARD EVENTS
	VirtualUSMAllInOneLite	40001											
	VirtualUSMStandardLogger	40001									Block		

Configure Log Forwarding

Next, you need to configure log forwarding on the USM Appliance Server or USM Appliance All-in-One.

To configure log forwarding

- Log into the USM Appliance Server web UI.
- Go to **Configuration > Deployment > Servers**.

You should now see both the USM Appliance Server and the USM Appliance Logger listed.

- Select the USM Appliance Logger and click **Modify**.
- On the next page, type the credentials for the **Remote Admin User** and the **Remote Password**.

These are the admin user credentials to log into the Logger.

- To populate the remote URL field automatically, click anywhere within the field.
- Click **Set Remote Key**.



Warning: Starting from version 5.5.1, the remote key cannot be empty. You need to use the same key on every USM Appliance Server connecting to the USM Appliance Logger. A warning displays if the key is not set. See [Prerequisites](#) for more details.

- Return to the Servers page, select the USM Appliance Server and click **Modify**.
- Set the option for **Log** to **No**.

9. In the Forward Servers section of the page, click **Add Server**.

This extends the form and displays a list labeled **Server**.

10. Select the USM Appliance Logger and click **Add New**.

The Logger and its IP address appears in the Server field.

11. Click **Save**.
12. Return to the Servers page, click **Apply Changes**.
13. To verify that you added the USM Appliance Logger successfully, click **Server Hierarchy**.

You should now see that there is an arrow extending from the USM Appliance Server to the USM Appliance Logger, where previously they were each floating freely in the graph.

DEPLOYMENT

COMPONENTS | **PLUGIN BUILDER** | **LOCATIONS**

ALIENVault CENTER | SENSORS | **SERVERS** | REMOTE INTERFACES

SHOW 20 ENTRIES CONNECT TO USM CENTRAL ADD SERVER DE

IP	NAME	PORT	SIEM	RISK ASSESSMENT	CORRELATION	CROSS CORRELATION	SQL STORAGE	ALARM SYSLOG	IP REP	LOGGER
	VirtualUSMAIInOneLite	40001	✓	✓	✓	✓	✓	✗	✓	✗
	VirtualUSMStandardLogger	40001	✗	✗	✗	✗	✗	✗	✗	✓

▼ **SERVER HIERARCHY**

```

graph LR
    A[VirtualUSMAIInOneLite ( )] --> B[VirtualUSMStandardLogger ( )]
  
```

The Logger becomes active immediately. To view logger activity on the USM Appliance Server or USM Appliance All-in-One, go to **Analysis > Raw Logs**.

Time frame selection GMT-5:00: **Last 2 Hours** | Last 24 Hours | Last Week | Last Month | All | Custom

VirtualUSMStandardLogger 1,451 logs

SHOW 50 ENTRIES PER SERVER TIME RANGE: 2018-02-23 14:00:00 <-> 2018-02-23 16:01:06 GMT-5:00

ID	SERVER	DATE GMT-5:00	TYPE	SENSOR	SOURCE	DESTINATION	DEVICE IP	DATA	EVENT NAM
1	VirtualUSMStandardLogger	2018-02-23 16:01:06	ssh	VirtualUSMStandardLogger	192.168.73.144:52507	192.168.73.166:22	192.168.73.166	Feb 23 16:01:06 VirtualUSMStandardLogger sshd[30417]: Accepted	[...] Validate
2	VirtualUSMStandardLogger	2018-02-23 16:01:06	AlienVault HIDS- authentication_success	VirtualUSMStandardLogger	192.168.73.166	192.168.73.166	192.168.73.166	AV - Alert - "1519419666" --> RID: "5501"; RL: "3"; RG: "pam,syslog,authentication	[...] Validate
3	VirtualUSMStandardLogger	2018-02-23 16:01:06	ssh	VirtualUSMStandardLogger	192.168.73.144:52510	192.168.73.166:22	192.168.73.166	Feb 23 16:01:06 VirtualUSMStandardLogger sshd[30424]: Accepted	[...] Validate



Note: The Server column displays the name of the USM Appliance Logger, indicating these events are not stored locally.

Checking System Status of the USM Appliance Logger

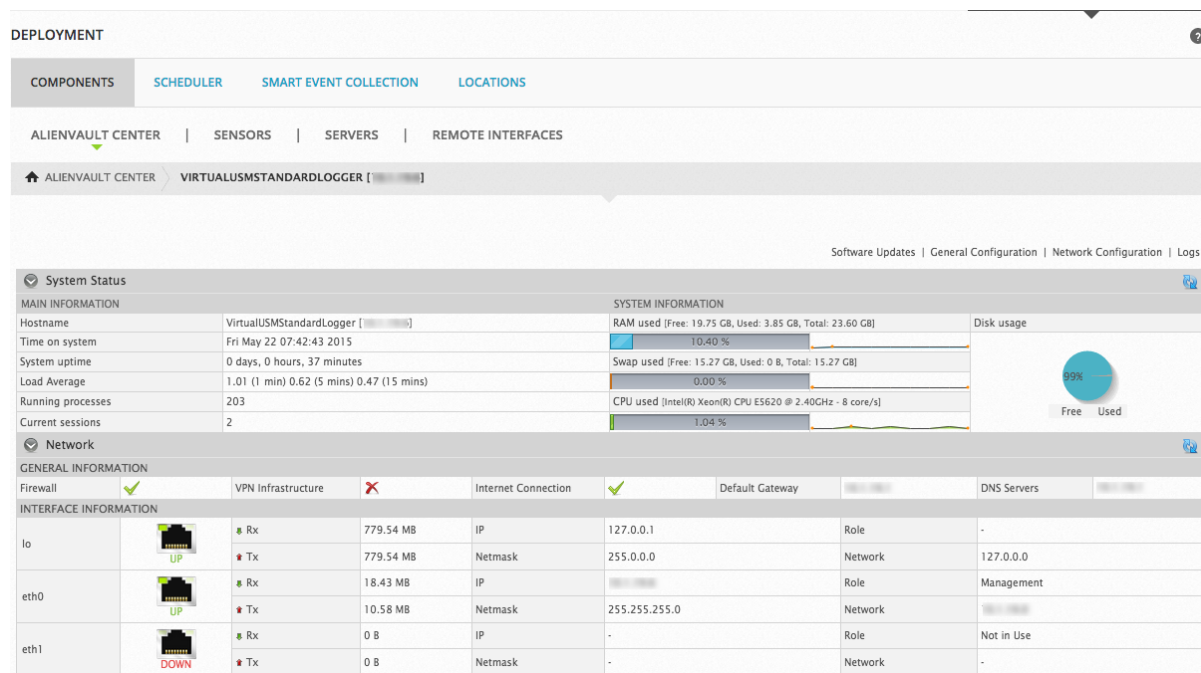
After the USM Appliance Logger starts receiving raw logs, it will fill up if left unattended. Therefore, AlienVault recommends that you check the system status of the USM Appliance Logger frequently. To determine how many events your USM Appliance Logger stores every day and how often you should check, refer to "Establishing Baseline Network Behavior" in the *USM Appliance User Guide*.

To check system details of the USM Appliance Logger

1. Log into the USM Appliance Logger using the web UI.
2. Go to **Configuration > Deployment > AlienVault Center**.
3. Double click the logger for which you want to check the status.

The System Details page of the logger displays, where you can find disk usage, as well as

RAM, Swap, and CPU usage:



In addition to checking the System Details page, USM Appliance issues a warning when the system has less than 25% or 10% of the total disk space available. You can find these warnings in the Message Center on the USM Appliance Logger.

Disk space is low ([REDACTED])

2015-05-22 07:22:07

The system has less than 25% of the total disk space available. Please address this issue soon to avoid a service disruption. At 2015-05-22 07:22:07.

- Clean cache of software updates:
 1. Go to *AlienVault console* (alienvault-setup)
 2. *Maintenance & Troubleshooting / Maintain Disk and Logs / Clear System Update Cache.*
- Purge old System logs:
 1. Go to *AlienVault console* (alienvault-setup)
 2. *Maintenance & Troubleshooting / Maintain Disk and Logs / Purge Old System Logs.*
- Adjust your [Backup options](#).

Configure the USM Appliance Enterprise Server and Enterprise Database

The AlienVault USM Appliance Enterprise Server component is hardware only, and ships with two devices: an Enterprise Server and an Enterprise Database.

The Enterprise Server needs to know the IP address and password of the Enterprise Database. Likewise, the Enterprise Database needs to know the IP address of the Enterprise Server. This information ensures that the two devices can communicate with each other.

Both configurations occur using the AlienVault Setup menu.

Task 1: Start the USM Appliance Enterprise Server Configuration

You should have already assigned an IP address to the Enterprise Server by following the procedure [Set Up the Management Interface](#).

To start the USM Appliance Enterprise Server configuration

1. On the AlienVault Setup menu, use the Tab key to go to **Configure Enterprise Server**; press **Enter** (<OK>).
2. When the AlienVault MySQL Setup menu appears, move it to the background temporarily while you proceed with configuring the USM Appliance Enterprise Database.

You will return to this later.

Task 2: Start the USM Appliance Enterprise Database Configuration

You should have already assigned an IP address to the Enterprise Database by following the procedure .

To configure the USM Appliance Enterprise Database

1. On the AlienVault Setup menu, use the Tab key to go to **Configure Database**; press **Enter** (<OK>).
2. On the **Configure Database** menu, use the Tab key to select **Configure AlienVault Server IP**; press **Enter** (<OK>).
3. In the **Enter Server IP Address** field, enter the IP address of the USM Appliance Enterprise Server; press **Enter** (<OK>).

The Configure Database menu appears again.

4. Use the Tab key to select **Configure AlienVault Framework IP**; press **Enter** (<OK>).
5. In the **Enter Framework IP Address** field, type the same IP address you did for the server in step 3.; press **Enter** (<OK>).

The application returns you to the Configure Database menu.

6. Select **Back** and press **Enter** until you progress back to the AlienVault Setup menu.

7. On the **AlienVault Setup** menu, use the Tab key to select **Apply all Changes**; select **OK**.

The application prompts you to confirm your choice.

8. Confirm by selecting **Yes**.

A progress screen appears showing you that the services are restarting and the percentage of job completion.

9. On the **Apply all Changes** screen, press **Enter** (<OK>).

10. On the **AlienVault Setup** menu, use the Tab key to select **Jailbreak System**; press **Enter** (<OK>).

The application prompts you to confirm your choice.

11. Enter the following command

```
grep ^pass /etc/ossim/ossim_setup.conf
```

12. Write down the password to be entered on the Enterprise Server.

13. Enter `exit` to return to the AlienVault Setup menu.

Task 3: Continue USM Appliance Enterprise Server Configuration

To continue the USM Appliance Enterprise Server configuration

1. On the **AlienVault MySQL Setup** menu, in the **Enter MySQL Server IP address** field, type the IP address of the USM Appliance Enterprise Database; press **Enter** (<OK>).
2. In the **Enter MySQL Server password** field, enter the password recorded from step [Write down the password to be entered on the Enterprise Server](#). above.



Note: The characters are invisible as you type the password.

3. Press **Enter** (<OK>) to finish the configuration.
4. On the **AlienVault Setup** menu, use the Tab key to select **Jailbreak System**; press **Enter** (<OK>).

The application prompts you to confirm your choice.


5. Type the following command

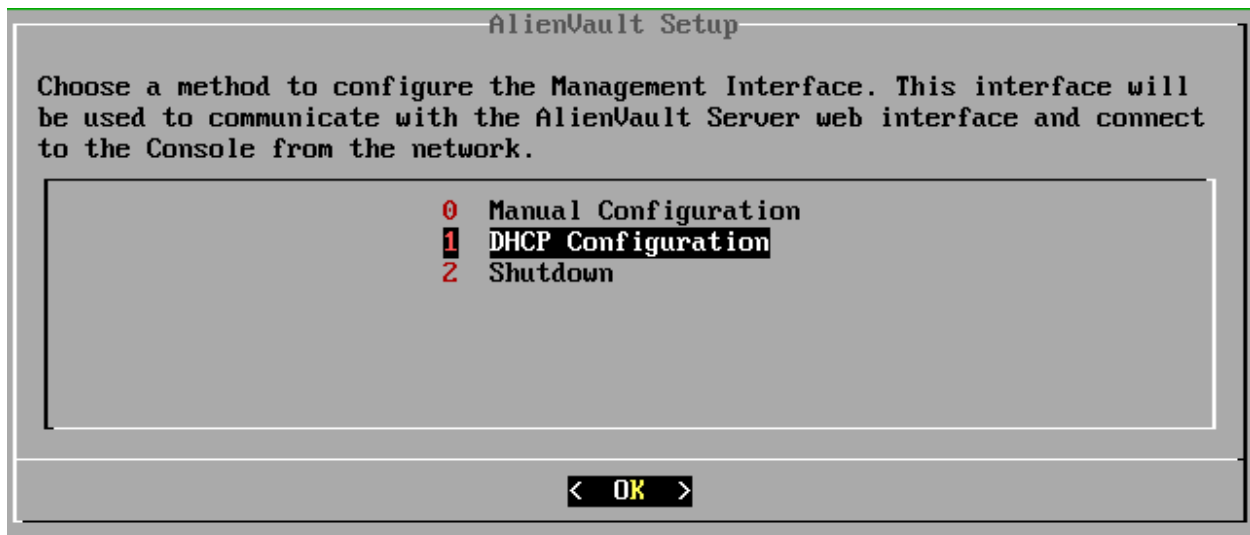
```
alienvault-api add_system --system-ip=<IP-of-Enterprise-Database>  
--password=<root-password-of-Enterprise-Database>
```

6. Type `exit` to return to the AlienVault Setup menu.

Set Up the Management Interface

The first time you power on the USM Appliance hardware or launch the virtual machine console after the deployment, you must configure the management interface to establish network connection. You can configure the management interface [manually](#) or use [DHCP](#) (Dynamic Host Configuration Protocol). But after the initial setup, DHCP configuration is no longer available.

 **Important:** When using DHCP configuration, you should create an address reservation for USM Appliance prior to configuration. To ensure proper functionality, USM Appliance requires a static IP address.



To configure the management interface using DHCP

1. On the AlienVault Setup screen, select **DHCP Configuration**.
2. USM Appliance displays the network settings assigned by your DHCP server. Press **Enter** to apply.

USM Appliance configures the management interface and AlienVault services.

To configure the management interface manually

1. On the AlienVault Setup screen, select **Manual Configuration**.
2. Type the **IP address** and press Enter.
3. Type the **Netmask** for the network and press Enter.
4. Type the **Gateway** for the network and press Enter.

5. Type the IP address of the **DNS server** and press Enter.



Note: If you have multiple DNS servers, type each of their IP addresses separated by a comma.

6. Verify the values you entered previously and press Enter.

USM Appliance configures the management interface and AlienVault services.

Register USM Appliance

You can register USM Appliance in one of three ways

Registering USM Appliance through the Web UI

With the exception of the USM Appliance Sensor, you can register USM Appliance through the web UI. USM Appliance Sensor registration must occur [through the AlienVault Console](#).

Prerequisites for Registration

- The appliance must have a connection to the Internet.
- You must have the USM Appliance license key issued by AlienVault.

To register through the web UI

1. Open a web browser and type the USM Appliance IP address into the address bar.

The AlienVault Free Trial Activation screen appears.

2. Click **click here** to enter your product license key.
3. On the welcome screen, type the license key in the **Product License Key** field and click **Send**.

An information box displays telling you that AlienVault USM Appliance activated successfully.

4. Click **Finish**.

The Welcome screen appears and contains a form that you must fill out to create the default admin account for the web UI. See [Create the Default Admin User](#) for details.

Registering USM Appliance from the AlienVault Console

USM Appliance Sensor registration must occur through the AlienVault Console. You can register other USM Appliance from the console as well.

Prerequisites for Registration

- The appliance must have a connection to the Internet.
- You must have the USM Appliance license key issued by AlienVault.

To register through the AlienVault Console

1. Log into the AlienVault Console.

The AlienVault Setup menu appears.

“Register this Appliance” is now the default selection.

2. Press Enter to register.
3. On the Online Registration screen, tab to **Online registration** and press **Enter**.
4. Type the license key, then press **Enter**.

The registration process can take several seconds. A status message displays a registration progress bar.

5. When registration has completed, message box displays:

```
AlienVault USM Appliance activated successfully.
```

6. To continue, press **Enter**.

The AlienVault Setup menu appears again, but this time *without* the Register this Appliance menu option.

Registering USM Appliance Offline

AlienVault recommends that you register USM Appliance using one of the online methods because it is easier and faster. However, if you do not have access to the Internet or you are in a confined environment, you can also register USM Appliance offline.

Prerequisites for Offline Registration

To register the appliance offline you must have the following:

- A license key file called `alienvault-license.deb` specific to each USM Appliance instance, obtained from AlienVault Technical Support.

Before AlienVault Support can generate and send you the license key file, you must first send them the `system_id` of each USM Appliance system that you want to register.

To find the `system_id` of your USM Appliance system

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

The AlienVault Setup menu displays.

- 1.

2. Select **About this Installation** and press Enter.
3. Copy the `system_id` from the screen and send it to [AlienVault Technical Support](#).

Registering USM Appliance Offline

To register offline using a USB flash drive

1. Save the license file you received from AlienVault, `alienvault-license.deb`, to a computer desktop or other location where you can easily retrieve it.
2. Insert a FAT32-formatted USB flash drive into the same computer, and then copy the license file to the root directory of the formatted USB flash drive.
3. Connect to USM Appliance through SSH.

The AlienVault Setup menu appears with "Register this Appliance" as the default selection.

4. Press Enter to register.
5. Select **Offline registration**.
6. Connect the flash drive to the USB port of the machine and press **Enter** (<OK>).

Your system will be registered after this process completes successfully.

Alternatively, you can choose to register USM Appliance offline without using the USB flash drive.

To register offline without a USB flash drive

1. Save the license file you received from AlienVault, `alienvault-license.deb`, to a computer desktop or other location where you can easily retrieve it.
2. Transfer the license file to USM Appliance directly using SCP.

For example, use the command below to copy `alienvault-license.deb` to the `/root` directory in USM Appliance

```
scp alienvault-license.deb root@<USM-Appliance-IP-address>:/root/
```

You will be prompted to enter the password for the root user of the USM Appliance instance.

3. Connect to USM Appliance through SSH.
4. 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.

5. Run the following command from the root directory, where the `alienvault-license.deb` file exists

```
dpkg -i alienvault-license.deb
```

Your system will be registered after this process completes successfully.

If you need to update the license key after registration, see [Update Your AlienVault License Key](#).

USM Appliance Initial Setup

Before performing the setup tasks, you must have successfully deployed USM Appliance and [Set Up the Management Interface](#). You also need to have access to the AlienVault Setup menu.

Topics covered in this section include the following:

Access the AlienVault Setup Menu	84
Configure Network Interfaces	86
Configure the Search Domain	89
Configure a Hostname for USM Appliance	90
Change the Default Time Zone	91
Configure USM Appliance to Use a DNS	92
Configure Synchronization with an NTP Server	92
Configure USM Appliance to Recognize Your Local Keyboard	93
Configure Custom HTTPS Certificates in USM Appliance	94
Create the Default Admin User	96
Configure Mail Relay in USM Appliance	97
Configure USM Appliance to Use a Proxy	100

Access the AlienVault Setup Menu

You can access the AlienVault Setup menu in one of the following ways:

- **Local Management** — By using a monitor, keyboard, and mouse connected directly to the USM Appliance hardware.
- **Virtual Management** — Virtual Appliance users access the console as a vSphere client or through an `SSH` client such as PuTTY.
- **Remote Management** — After IPMI or HPE iLO configuration, you can access the console by any computer connected to the same subnet in which the appliance runs, through the remote connection.

For procedural simplicity, the following task steps reference the user interface (UI) of the `SSH` client PuTTY as means to explain how to access the AlienVault console.

To access the AlienVault console

1. Launch PuTTY or any other `SSH` client, and in the **Host Name (or IP address)** field, type the IP address of the appliance.
2. Make sure that `SSH` is selected.

This is usually the default setting.
3. Click **Open**.
4. Enter the user credentials you use to log into the `SSH` client.

The AlienVault splash screen for USM Appliance appears. If this is the first time, it displays the root username and a randomly generated password for you to enter.


```


=====
===== http://www.alienvault.com =====
=====
===  Access the AlienVault web interface using the following URL:  ===
=====
===== https://10.1.23.5/ =====
=====
= ##### First time instructions #####
= 1. Enter USERNAME:root and PASSWORD:znuffxvu to access
= 2. You will be prompted to change this password in the first run *only*
= 3. Enjoy!

AlienVault USM [redacted] - x86_64 - tty1
VirtualUSMStandardServer login:  ←

```


5. In the **login:** field, enter `root`.
6. In the **password** field, enter the displayed randomly generated password, then press **Enter**.
7. When prompted whether you would like to change your password, click **Yes**.

After initial login using the default username and randomly generated password, USM Appliance prompts you to change the password.

 **Important:** If you want to configure high availability (HA) for a USM Appliance Standard or Enterprise component, you must give both the primary and secondary node the same root password. See [High Availability Configuration](#).

To change the root password

1. On the first **Change Root Password** panel, type your new password in the **New root password** field and press **Enter**.

 **Note:** The cursor is not visible on the field. To verify that your cursor is in the right location, look for a black left border at the start of the field. This tells you that your cursor is where it should be.

2. On the second **Change Root Password** panel, type the password you entered previously and press **Enter**.

3. On the third, and final, **Change Root Password** panel, a confirmation message appears, showing that you have successfully updated the password.

The application now prompts you to log in again, using the newly created password.

Configure Network Interfaces

USM Appliance All-in-One comes with six network interfaces, numbered `eth0` to `eth5`. USM Appliance uses these interfaces to perform the following functions:

- Connect to the Internet
- Monitor the network, using its built-in IDS capabilities
- Run asset scans
- Collect log data from your assets
- Run vulnerability scans
- Generate network flows

Based on functionality, you can classify the interfaces into the following categories:

Management

By default, USM Appliance uses the management interface to perform network monitoring, log collection, and scanning. So, for this reason, you do not need to configure any additional interfaces, *as long as they are all on the same subnet as the management interface*.

The management interface lets you communicate with the AlienVault console, as well as connect to the web UI.



Note: The default port for the management interface is `eth0`. However, you may configure a different port for this interface, if desired.

Network Monitoring

When the administrator configures an interface for network monitoring, the interface operates in passive listening mode (also known as *promiscuous* mode). A network tap or span is set up that allows the interface to monitor all packet traffic passing through it for threats.

Because USM Appliance's built-in IDS capability uses the network monitoring interface, you must dedicate at least one of the network interfaces to it.

Log Collection and Scanning

You use the Log Collection and Scanning interface to reach the networks and systems from which you want to collect data. You also use it to scan the systems, using USM Appliance's built-in asset discovery, vulnerability assessment, and availability monitoring tools.

Setting up this interface requires assignment of an IP address and network mask to the interface.

Not in Use

This is the default option for all the interfaces except the management interface. It applies to any network interface that is not in use and not configured.

Update Management Interface Configuration

You must configure the management interface immediately after deploying the USM Appliance virtual machine or the first time when you power on the USM Appliance hardware. See [Set Up the Management Interface](#) for details.

If you need to modify the management interface configuration, 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 **Configure Network**.
4. Select **Setup Management Network**.
5. Use the keyboard arrow keys to move to the interface, select the interface by pressing the spacebar, and then press Enter (<OK>).
6. Type the **IP address** and press Enter.
7. Type the **Netmask** for the network and press Enter.
8. Type the **Gateway** for the network and press Enter.
9. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
10. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Configure Additional Network Interfaces

In addition to providing network connection, the management interface on USM Appliance can also monitor your network and collect logs from your assets. But if you want to use a different interface with a different IP address to perform those functions, you must configure those interfaces separately.

To set up additional network interface

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 **Configure Network**.
4. Select **Setup Network Interface**.
5. Use the keyboard arrow keys to move to the interface, select the interface by pressing the spacebar, and then press Enter (<OK>).
6. Type the **IP address** and press Enter.
7. Type the **Netmask** for the network and press Enter.
8. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
9. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

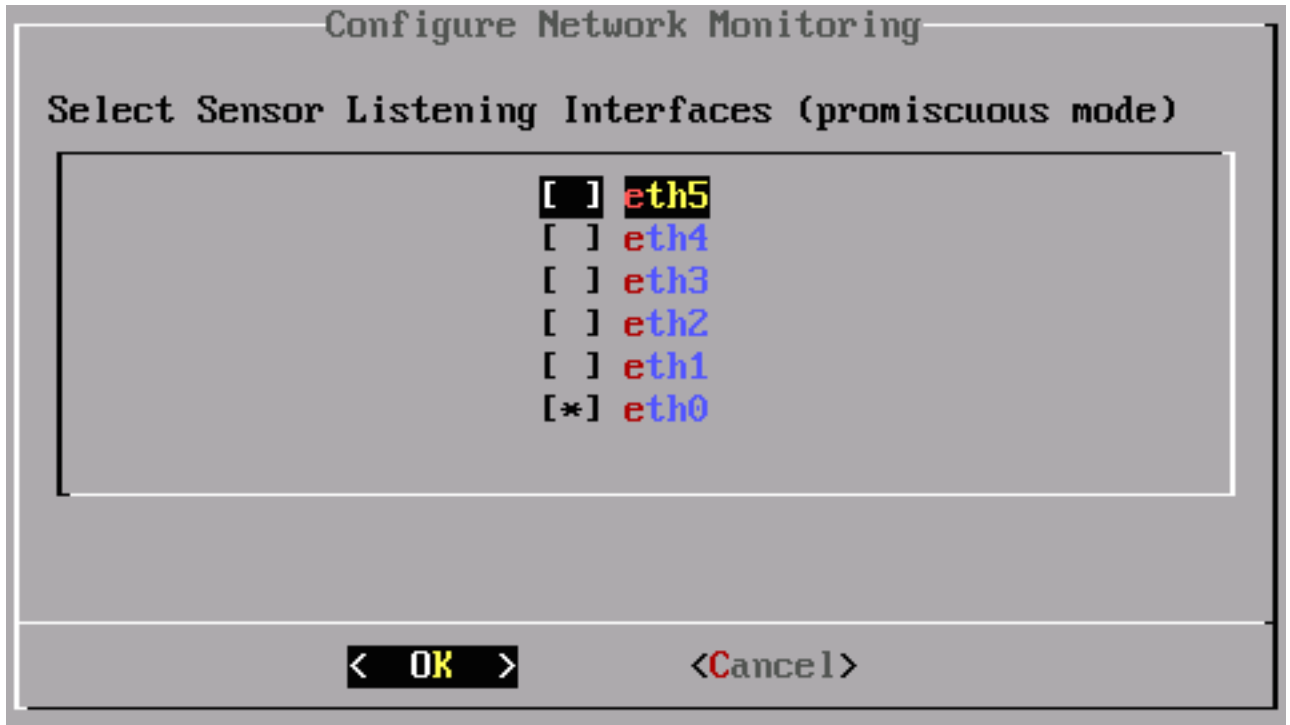
Enable Additional Listening Interfaces

If you want to use different interfaces to monitor network traffic but do not want to assign IP addresses to them, you can enable them in promiscuous mode.

To enable additional listening interfaces on USM Appliance All-in-One or USM Appliance Sensor

1. Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
2. Select **Configure Sensor**.
3. Select **Configure Network Monitoring**.

4. Use the keyboard arrow keys to move to the interface, select the interface by pressing the spacebar, and then press Enter (<OK>).



5. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
6. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Configure the Search Domain

For DNS (Domain Name System) lookup and reverse DNS resolution to work correctly, USM Appliance requires that you configure the search domain after you have completed the deployment.

To configure the search domain in USM Appliance

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 **Configure Network**.

4. Select **Network Domain**.
5. Type the domain name of your network and press Enter. The default is `alienvault`.



Important: You can only enter ONE domain in this field.

6. Press Enter to continue.
7. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
8. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

9. Return to the AlienVault Setup main menu and select **Reboot Appliance**.

Configure a Hostname for USM Appliance

You should always configure a hostname for USM Appliance. This helps you identify each one uniquely, which is particularly important if you need to contact AlienVault Support for technical assistance.

Your PCI DSS 3.1 compliance audit will fail when a certificate whose Common Name (CN) or whose entries in the X509 Subject Alternative Name do not match the Fully Qualified Domain Name (FQDN) of the system in AlienVault USM Appliance.

Certificates, whose CN is not equal to the FQDN, cannot be verified through a Public Key Infrastructure (PKI). A service using such a certificate cannot authenticate itself towards a user, unless the user can determine its trustworthiness through another channel. If there is no additional channel available, a user cannot distinguish between a genuine and a forged certificate, which benefits the man-in-the-middle attack.

Therefore, AlienVault recommends that you use the FQDN when naming USM Appliance and to also use this FQDN as the CN or as X509 Subject Alternative Name (type DNS) to reduce the risk of man-in-the-middle attacks and to avoid failure in PCI compliance audits.

To configure a hostname for USM Appliance

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 **Configure Hostname**.

4. Type the name for this host and press Enter.



Note: Any name you choose must not have spaces in it. For guidance on choosing a name, see [RFC 1178](#).

5. Press Enter to continue.
6. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
7. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

8. Return to the AlienVault Setup main menu and select **Reboot Appliance**.

Change the Default Time Zone

The default time zone for USM Appliance is Pacific Time (UTC -7h). If you are not operating in that time zone, you must change it. Otherwise, USM Appliance does not accurately timestamp events.

To change the default time zone

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 Location**.
4. Select **Date and Time**.
5. Select **Configure Time Zone**.

An information panel advises you that the time zone, as well as your profile and the mysql services, will be changed.

6. Press Enter to confirm.

The Package Configuration panel appears, where America is the default setting.

7. Locate the applicable region or continent for your location.
8. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.

9. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Configure USM Appliance to Use a DNS

Use of a Domain Name Service (DNS) helps USM Appliance to resolve host names against IP addresses. When processing logs from different assets, or hosts, to generate events, if the IP address of the asset can be identified, USM Appliance stores it in the Device IP field of the event. This enriches the event data, making searches faster and more accurate. When USM Appliance is not able to resolve the host name, it assigns the IP address of the USM Appliance Sensor to the Device IP field instead.

To configure USM Appliance to use a DNS

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 **Configure Network**.
4. Select **Name Server (DNS)**.
5. Type the IP address of the server you want to use. If using more than one server, separate them with a comma without any spaces. For example:

```
1.1.1.1,8.8.8.8
```

6. Press Enter (<OK>).
7. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
8. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Configure Synchronization with an NTP Server

Use of an NTP server in your network helps ensure that all system components are correctly synchronized. This is particularly important for timestamp accuracy and auditability in your efforts to comply with certain regulatory standards.

If you plan to configure high availability (HA) in a USM Appliance Standard or Enterprise deployment you must set up one NTP server for your primary nodes and another for your secondary nodes, and synchronize each node to its respective NTP server. See [High Availability Configuration](#).



Important: The NTP server requires use of port 123 over UDP.

To enable or disable synchronization with an NTP server

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 Location**.
4. Select **Date and Time**.
5. Select **Configure NTP Server**.
6. Select **Enable** by pressing the spacebar, and then press Enter (<OK>).
7. Type the hostname or IP address of the NTP Server.

The application returns you to the Date and Time menu.

8. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
9. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Configure USM Appliance to Recognize Your Local Keyboard

Follow this procedure if your keyboard does not use a United States key layout.

To change the default keyboard layout

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 Location**.

4. Select **Configure Keyboard**.
5. Use the keyboard arrow keys to scroll the list and find your selection, and then press Enter (<OK>).

You will be able to select the Keyboard model, Keyboard layout, Key to function as AltGr, and Compose key.

6. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
7. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Configure Custom HTTPS Certificates in USM Appliance

You can secure USM Appliance by providing your own SSL certificates from a Certificate Authority (CA), and you can upload them through the web UI.

To upload a custom HTTPS certificate in USM Appliance

1. Log into the USM Appliance web UI and go to **Configuration > Administration > Main**.
2. Extend **USM Framework**.
3. Click the **Browse** button to upload your custom web server SSL certificate and private key files in Privacy Enhanced Mail (PEM) format:



Important: Make sure that your certificate file includes both the "begin" and "end"



lines.

4. (Optional) If your SSL certificate requires any intermediate certificates, upload it in **Web Server SSL CA Certificates (PEM format)**.

If you need help generating a certificate, see [How to Generate a Certificate Signing Request for USM Appliance](#).

Convert Certificates to PEM Format

USM Appliance only accepts certificates in the PEM format, which is the most common format that certificates are issued. However, different operating systems (OSes) generate certificates in different formats. For example, Windows OS typically produce certificates in PFX or PKCS#12 format, with extensions `.pfx` or `.p12`.

If your certificate is not in the PEM format, you can use OpenSSL to convert it. OpenSSL is installed on USM Appliance by default. The following procedure illustrates how to convert a certificate from PFX to PEM format using USM Appliance.

To convert your certificate to the PEM format

1. Obtain a certificate from your CA.
2. Upload your certificate file to USM Appliance.



Note: For example, Linux and macOS users can use the `scp` command while Windows users can use a program called WinSCP.

3. Connect to the AlienVault Console through `SSH` and use your credentials to log in.
4. On the AlienVault Setup main menu, select **Jailbreak System** to gain command line access.
5. Generate the following files:

- a. Certificate:

```
openssl pkcs12 -nokeys -nodes -in certificate.pfx -out av_
certificate.pem
```

- b. Private key:

```
openssl pkcs12 -nocerts -nodes -in certificate.pfx -out av_private_
key.pem
```

- c. CA certificate chain (optional):

```
openssl pkcs12 -cacerts -nokeys -in certificate.pfx -out av_ca_certificate_chain.pem
```

6. Edit the files to remove any extra lines. You can use *vim* or *nano* as editors.



Note: Certificate files have -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- while private key files have -----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY----- surrounding the content. You need to remove any extra lines above or below these texts.

7. Download the new certificate files to your desktop.
8. Log into the USM Appliance web UI and go to **Configuration > Administration > Main**.
9. Extend **USM Framework**.
10. If you have configured a certificate in the past, click **Remove** to delete the old certificate, and then **Update Configuration** to apply the changes.

Allow 2-5 minutes for reconfiguration to run in the background. After the web browser refreshes, you may receive a warning about custom self-signed certificate in use. You can ignore this message.

11. Browse to and upload the certificate files generated in step #5.
12. Verify that the new certificate is installed and ready to be used.

Create the Default Admin User

When you connect to the USM Appliance web UI for the first time after installation and setup, USM Appliance prompts you to create the *default admin* user.

After you create the default admin, you can log in and use USM Appliance.

To create the default admin

1. Access the USM Appliance web UI.

The Welcome screen appears when you access the web UI for the first time.

The screenshot shows the 'Welcome' screen of the USM Appliance web UI. It includes a message congratulating the user for choosing AlienVault and instructing them to create an administrator user account. Below this is the 'Administrator Account Creation' section, which contains a form with the following fields: FULL NAME *, USERNAME *, PASSWORD *, CONFIRM PASSWORD *, E-MAIL *, COMPANY NAME, and LOCATION. The USERNAME field is pre-filled with 'admin'. A blue button labeled 'START USING ALIENVAULT' is at the bottom of the form. A link for 'View Map' is next to the LOCATION field.

2. Fill out the form.
3. When you finish filling out the form, click **Start Using AlienVault**.
4. Type the admin username and password you created in the form, then click **Login**.

If you plan to have multiple administrators to help administer USM Appliance, you should create one or more *admin* users.

For instructions to create additional administrators locally on USM Appliance, see "Creating New Accounts for Local Users" or to create additional administrators using LDAP, see "Creating New Accounts for LDAP Users" under User Administration in the *USM Appliance User Guide*.

Configure Mail Relay in USM Appliance

You can configure to receive emails from USM Appliance. For example, if you want to receive an email when an alarm appears, you can create a policy for the email to be sent. For details, see [Tutorial: Create a Policy to Send Emails Triggered by Events](#). But first, you need to configure mail relay in USM Appliance.

USM Appliance uses *Postfix*, an open-source mail transfer agent (MTA), as Simple Mail Transfer Protocol (SMTP) server for outgoing messages.

USM Appliance SMTP Server Default Settings

Protocol	Port Number	Notes
SMTP	25	This is the port number assigned to SMTP and used for mail server relay. Note that most Internet service providers (ISPs) block this port to curb the amount of spam they receive.
TLS (Transport Layer Security)	587	This is the default port number that USM Appliance uses to send outgoing messages. The connection is encrypted by executing the <code>STARTTLS</code> command.

USM Appliance also enables the following properties from Postfix:

```
smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
```


This means USM Appliance enables Simple Authentication and Security Layer (SASL) authentication for SMTP, denying anonymous authentication.

Mail Server Relay Configuration

For simply receiving emails from USM Appliance, you do not need to set up mail server relay. However, if your company has a dedicated mail server that you want to keep using, you can configure USM Appliance to route emails through your corporate mail program. To prevent such messages from going to your junk mail or spam folder, you can [add USM Appliance as a safe sender for Office 365](#) or [add it to the email whitelist for Gmail](#).

You perform this task on either a USM Appliance All-in-One or a USM Appliance Server.

To configure mail server relay on USM Appliance

1. Log in to the USM Appliance web UI, and then go to **Configuration > Deployment**.
2. Under AlienVault Components Information, click the  icon of the system you want to change.
3. On the next page, click **General Configuration**, located above the System Status.
4. In the General Configuration form, select **Yes** for Mail Server Relay.

This expands the form to disclose new fields.

5. Enter the Server IP, the username and password used for the mail server, and the port number in the respective fields.



Note: The Server IP field accepts valid IP addresses or server names.

For Gmail:

- **Server IP:** smtp.gmail.com
- **User:** <your user>@gmail.com or <your user>@<your domain>.tld if <your domain>.tld is managed by Google Professional Services
- **Pass/Confirm Pass:** <your password>
- **Port:** 587

For Office 365:



Note: If your Office 365 admin has set up two-step verification for your organization, you may need to [create an app password allowing USM Appliance to access your Office 365 account](#).

- **Server IP:** smtp.office365.com
- **User:** <your user>
- **Pass/Confirm Pass:** <your password>
- **Port:** 587

For Exchange Server 2013:



Important: Before continuing, follow the steps in [How to Configure a Relay Connector in Exchange Server 2013](#) to allow SMTP relay through the Front End Transport service.

- **Server IP:** <your Exchange Server 2013 IP address>
 - **User:** (leave it blank)
 - **Pass/Confirm Pass:** (leave it blank)
 - **Port:** 25 (default)
6. Click **Apply Changes**.
 7. (Optional) If you want to change the sender's email address (default is no-reply@alienvault.com), go to **Configuration > Administration > Main**.
 8. Extend **USM Framework** and update **Sender's Email Address for Notification**.



Note: USM Appliance uses this email address to send notifications in the following occasions:

- A report is distributed via email.
- USM Appliance informs you about open tickets.
- USM Appliance creates a ticket based on a vulnerability it discovers.
- A comment has been added to or modified in an existing ticket.

9. Click **Update Configuration** to apply the changes.

Configure USM Appliance to Use a Proxy

By default, USM Appliance does not need to go through any proxy server, so proxy configuration is disabled. However, should you need to use a proxy in your environment, USM Appliance provides two options: manual (external) and alienvault-proxy (built-in), for proxy configuration.

Manual Proxy Configuration

If your company requires all network traffic to go through a proxy server before reaching the Internet, you can configure the proxy in USM Appliance.

To configure USM Appliance to use an external proxy

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 **Configure Network**.

4. Select **Proxy Configuration**.
5. Click **manual**, or move the cursor to **manual** then press the spacebar, to make your selection.
6. Type the user name for the proxy.
7. Type the password for the proxy user. The password will not be displayed.
8. Type the port number used by the proxy.
9. Type the IP address or hostname of the proxy.
10. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
11. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

alienvault-proxy Proxy Configuration

Additionally, USM Appliance includes a built-in proxy that you may find useful, especially if you have more than one USM Appliance deployed. You can dedicate a USM Appliance All-in-One or USM Appliance Server to be the proxy server and the other USM Appliance instances will go through it to reach the Internet. For example, you can use this setup to control how updates are received from AlienVault. Only the dedicated USM Appliance (the proxy) downloads the updates from AlienVault, the other instances download the updates from the proxy instead, increasing performance and security.



You need to perform the same configuration in every USM Appliance instance deployed in your network.

To configure USM Appliance to use its built-in proxy

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 **Configure Network**.
4. Select **Proxy Configuration**.
5. Click **alienvault-proxy**, or move the cursor to **alienvault-proxy** then press the spacebar, to make your selection.
6. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.

7. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Getting Started Wizard

AlienVault provides a Getting Started Wizard for USM Appliance All-in-One to help first-time users configure the built-in security capabilities. Within minutes, the wizard walks you through a simple, step-by-step workflow to accomplish the following:

- Set up networks
- Run an asset discovery scan
- Deploy HIDS agents
- Configure external data sources

This section covers the following subtopics:

Running the Getting Started Wizard	104
Skipping the Getting Started Wizard	104
Configuring Network Interfaces	105
Discovering Assets in Your Network	108
Deploying HIDS to Servers	112
Enabling Log Management	116
Connecting to AlienVault Open Threat Exchange®	118

Running the Getting Started Wizard



Welcome to the AlienVault USM Getting Started Wizard

You are about to use this wizard to configure the critical security capabilities provided by AlienVault USM.



Once done you'll be ready to use AlienVault USM. Now, go forth!

[Skip AlienVault Wizard](#)

[START](#)

To run the Getting Started Wizard

- Click **Start** on the welcome page

We recommend that you perform the tasks in the listed order, because you will not be able to configure certain tasks before the previous one is completed.

Skipping the Getting Started Wizard

Running the Getting Started Wizard is highly recommended, but optional.

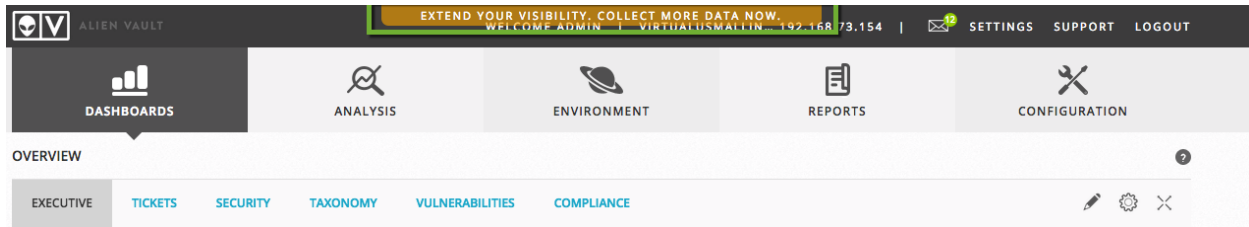
To skip it at any time, click **Skip AlienVault Wizard** on the Welcome page (shown), or subsequent pages.

If you skip the wizard, each time you log in as administrator, a banner appears above the primary navigation bar that reads:

Extend your visibility. Collect more data now.

Clicking this banner relaunches the Getting Started Wizard.

Until you click **Finish**, after completing the last task in the wizard, the reminder banner will be available.



Configuring Network Interfaces

An AlienVault USM Appliance All-in-One comes with six network interfaces, numbered `eth0` to `eth5`. USM Appliance uses these interfaces to perform the following functions:

- Monitor the network, using its built-in IDS capabilities
- Run asset scans
- Collect log data from your assets
- Run vulnerability scans
- Generate network flows

The interfaces include the options described in the following subtopics.

Management

By default, USM Appliance configures the management interface to perform network monitoring, log collection and scanning. So, for this reason, you do not need to configure any additional interfaces, *as long as they are all on the same subnet as the management interface*.

The management interface lets you

- Communicate with the AlienVault console
- Connect to the web interface

You cannot configure the management interface from the Getting Started Wizard; it is configured during initial setup from the AlienVault console. For more information, see [Set Up the Management Interface](#).



Note: The default port for the management interface is `eth0`. However, you may configure a different port for this interface, if desired.

Network Monitoring

When the administrator configures an interface for network monitoring, the interface operates in passive listening mode (also known as *promiscuous* mode). A network tap or span is set up that allows the interface to monitor all packet traffic passing through it for threats.

Because USM Appliance's built-in IDS capability uses the network monitoring interface, you must dedicate at least one of the network interfaces to it.

Log Collection and Scanning

You use the Log Collection and Scanning interface to reach the networks and systems from which you want to collect data. You also use it to scan the systems, using USM Appliance's built-in asset discovery, vulnerability assessment, and availability monitoring tools.

Setting up this interface requires assignment of an IP address and network mask to the interface.

Not in Use

This is the default option for all the interfaces except the management interface. This applies to any network interface that is not in use and not configured.

To configure network monitoring

1. Choose the network interface you want to use for network monitoring
2. Select **Network Monitoring** from the list.




Once selected, USM Appliance immediately configures the network interface to listen for

incoming traffic.

3. Configure your virtual machine to get traffic from your physical network.

Configure Network Interfaces

The network interfaces in AlienVault USM can be configured to run Network Monitoring or as Log Collection & interfaces you'll need to ensure that the networking is configured appropriately for each interface so that Alier or has the ability to reach out to the desired network.

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management ▼	192.168.73.155	-
eth1	Network Monitoring ▼	N/A	
eth2	Log Collection & Scanning ▼	172.16.1.12 	-
eth3	Network Monitoring ▼	N/A	
eth4	Not in Use ▼	N/A	-
eth5	Not in Use ▼	N/A	-

Once the network is forwarding data to the selected network interface, the **Status** indicator changes from red to green. This means that the interface is both configured and receiving data as expected.

After you've configured the network monitoring interface, verify that it's receiving network traffic. If you are on a virtual network, make sure that you are receiving network traffic and not just virtual switch traffic. Follow the instructions in [Monitor VMware Standard Virtual Switches](#).

To configure log collection and scanning

1. Choose the network interface that will be used for log collection and scanning.
2. Select "Log Collection & Scanning" from the list.

A screen pops up asking for an IP address and netmask. This information will be used to configure the network interface with a static IP address.

3. On the **IP Address & Netmask** box, enter an IP address and netmask for a different subnet.

The Configure Network Interfaces screen displays again. The IP address you supplied shows as the IP address for the interface. This indicates that the interface configuration is successful.

4. Configure the other interfaces as needed for additional log collection and scanning.



Note: In some situations the network that you want to monitor may not be accessible from the IP address provided without setting up a route in the routing table. This is an extreme case and should not happen often. If a route is required, you will need to jailbreak the system using the AlienVault console and configure the route using the command line.

After you have finished configuring the network interfaces, click **Next** at the bottom-right corner to proceed.

Discovering Assets in Your Network

Understanding what is in your environment is a critical step towards identifying threats and vulnerabilities.

When you complete the Asset Discovery task in the Getting Started Wizard, you can use the built-in asset discovery capability to do the following:

- Scan your networks and find assets
- Manually enter assets
- Import assets from a CSV file



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*.

Scan & Add Assets

In order to begin monitoring your environment we must first find the assets in your network. There are three (3) ways you can add assets to monitor: you can scan your network using network ranges, import a CSV of assets in your network, or you can add assets manually.

Add Asset Manually Option 3

Select an Asset Type ▼
+ ADD

Option 1

SCAN NETWORKS

Option 2

IMPORT FROM CSV

HOSTNAME	IP	TYPE	
Host-192-168-200-200	192.168.200.200	Select an Asset Type ▼	🗑️
Host-192-168-73-1	192.168.73.1	Select an Asset Type ▼	🗑️
Host-192-168-73-120	192.168.73.120	Windows ✕ ▼	🗑️
Host-192-168-73-2	192.168.73.2	Select an Asset Type ▼	🗑️
VirtualUSMAllInOne	192.168.73.154	Linux ✕ ▼	🗑️

SHOWING 1 TO 5 OF 5 ASSETS

FIRST
PREVIOUS
1
NEXT
LAST

Option 1: Scan Networks to Find Assets

This task informs AlienVault USM Appliance about the network topology. This enables you to successfully run asset scans, vulnerability scans, and use other built-in capabilities.

To scan your networks for asset discovery

1. From the Asset Discovery page of the Getting Started Wizard, click **Scan Networks**.
2. On the **Scan Networks** page, choose one or more networks to scan.

Scan Networks

The discovery scan will first ping your assets, then probe the services to identify operating system. Add networks manually or import networks from a CSV, if you do not see the networks you would like to scan.

SCAN NETWORKS

Add Networks

Network Name CIDR Description + ADD

Search

NETWORK NAME	CIDR	# OF POSSIBLE ASSETS	DESCRIPTION
<input checked="" type="checkbox"/> Local_192_168_73_0_24	192.168.73.0/24	256	
<input type="checkbox"/> test	10.1.2.0/24	256	test

SHOWING 1 TO 2 OF 2 NETWORKS FIRST PREVIOUS 1 NEXT LAST

IMPORT FROM CSV

CANCEL SCAN NOW

You should already have one or more networks defined, based on either the default management interface or on any additional networks that you defined that were not on the same subnet. See [Configuring Network Interfaces](#).

If you do not see the desired network, you can add or import them on this page, see [Adding More Networks Manually](#) or [Importing Networks From a CSV File](#), respectively.

3. Click **Scan Now**.

The confirmation page displays the number of assets that can be scanned, based on the network defined.

4. Confirm the asset scan by clicking **Accept**.



Note: If you created a large network (for example, 10.10.10.0/16), the scan may take a long time. We suggest that you create smaller networks. You can stop the scan while it is running, but no asset data will be retained if you do so, and you must run the scan again.

5. After the scan has finished, USM Appliance prompts you to schedule a recurring scan. This periodic scan helps you discover any changes in the environment promptly.

The default is a weekly scan.

6. To change the frequency to either daily or monthly, expand the list box. To select no scan, click the "x."
7. Click **OK** to accept and continue.

Adding More Networks Manually

To add more networks manually

1. On the **Scan Networks** page, type a meaningful name into the **Add Networks** field to describe the network, for example, DMZ or Employee Office.
2. Type the CIDR notation for the network.
3. (Optional) Type a description for the network to distinguish it, if helpful.
4. Click **+Add**.



Note: If you make a mistake and define the network incorrectly, use the delete icon (trash icon) to delete and re-enter the network.

Importing Networks From a CSV File

To import networks from a CSV file



Note: Pay attention to the formats allowed in the CSV files. The CIDR field is required. It can be a comma-separated list. The delimiter for the columns is a semicolon.

1. Click **Import from CSV** to display more options.
2. Click **Choose File** and select a CSV file.
3. Click **Import** to upload the selected file.

Option 2: Import Assets from a CSV File

You can also import a list of assets from a CSV file.

To import assets from a CSV file

1. Click **Import from CSV**.

The Import Assets from CSV popup appears.

2. Click **Choose File** and select a CSV file.
3. Click **Import** to upload the selected file.

A confirmation screen displays showing the number of hosts that have been imported.

Option 3: Add Assets Manually

If you do not have access to a list of assets in the form of a CSV file, you can quickly add them manually.

To add an asset manually

1. On the Scan & Add Assets page, type a meaningful name for the asset (for example, domain controller).
2. Type the IP address in the field provided.
3. Choose the asset type from the list.
4. Click **+Add**.
5. After you have finished adding all the assets, click **Next** at the bottom-right corner to proceed.

Deploying HIDS to Servers

We recommend deploying a host-based intrusion detection system (HIDS) to enable

- File integrity monitoring
- Rootkit detection
- Event log collection

The Getting Started Wizard provides two options for HIDS agent deployment.

Windows — HIDS agent is installed locally on specified hosts. All Windows hosts must meet the prerequisites described in the Asset Management topic, Deploying HIDS Agents, of the *USM Appliance User Guide*.

UNIX/Linux — HIDS agents are not installed on hosts but provide agentless operation. UNIX and Linux systems are monitored remotely for file integrity only. For information on installing HIDS agents on UNIX/Linux hosts, see [Deploy the AlienVault HIDS Agents to Linux 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 whitelist. 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 NTLMSPPP based (including secure RPC) clients**, select
 - Require NTLMv2 session security
 - Require 128-bit encryption
 - b. **Network Security: Minimum session security for NTLMSPPP 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 whitelist the IP address of USM Appliance, or temporarily disable the antivirus software during the installation.

To deploy HIDS

1. Select the **Windows** or the **UNIX/Linux** tab, as appropriate.
2. Type your **Username** and **Password**.



Note: For UNIX/Linux systems, this should be your `SSH` credentials.

3. (Windows only) Optionally, enter the **Domain** information.
4. From the asset tree on the right, choose the asset(s) on which you would like to deploy a HIDS agent.
5. Click **Deploy**.

The HIDS Deployment popup prompts you for confirmation

6. Click **Continue**.

A progress bar appears.

After the deployment finishes, a message displays the number of devices successfully deployed with HIDS.

7. Click **OK**.

Deploy HIDS to Servers

For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.

WINDOWS (1) **UNIX / LINUX (2)**

Enter the domain admin account to install the HIDS agent. The username and password you provide will *not* be permanently stored, it will be used to deploy an agent to the selected assets.

Username
ossec_agent

Password
.....

Domain (Optional)

DEPLOY

Asset tree

Deploy to the following hosts:

- Local_192_168_73_0_24
- Host-192-168-73-120

8. After you finish deploying the HIDS agents, click **Next** at bottom-right to proceed.

Enabling Log Management

One of the key capabilities provided by USM Appliance is the ability to collect external data from network devices, security devices, and your servers. The data collected allows USM Appliance to correlate events to see patterns of activity and issue alarms.

The Getting Started Wizard makes it painless and fast to configure each of the assets you discovered or added as part of the Asset Discovery task with the appropriate data collection plugin.



Note: You cannot collect data from those assets that do not have a plugin enabled. See [Enable Plugins](#) for more information.

On the Log Management page in the Getting Started Wizard, you will see a list of the network devices discovered as part of the [Configuring Network Interfaces](#) task. You should enable one or more plugins for each of these assets.

To enable plugins for each asset

1. Select the correct **Vendor**, **Model**, and **Version number** corresponding to the data that you want to collect from that asset.

All three fields are required. The Version field defaults to ‘-’ if no other selection is available. The **Add Plugin** button is enabled.

2. If you want to enable another plugin for the same asset, click **Add Plugin**.

Another row is added for you to select the Vendor, Model, and Version number for a different plugin.

3. Repeat step 1 and 2 for each plugin you want to enable. You can enable up to 10 plugins per asset.

Set up Log Management

During the asset discovery scan we found 2 network devices on your network. Confirm the vendor, model, and version of the device shown. Click the "Enable" button to enable the data source plugin for each device.

ASSET	VENDOR	MODEL	VERSION	
Host-192-168-73-2 (192.168.73.2)	Cisco ✕ ▼	ASA Adaptive Se... ✕ ▼	- ✕ ▼	✕
	Citrix ✕ ▼	NetScaler ✕ ▼	- ✕ ▼	✕
ADD PLUGIN				
Host-192-168-73-155 (192.168.73.155)	Select Vendor ▼	Select Model ▼	Select Version ▼	✕
	ADD PLUGIN			





ENABLE

4. Repeat step 1-3 for each asset.
5. To enable the selected plugins, click **Enable**.

The Log Management Confirmation page, shown in the following illustration, displays the plugins that you enabled. The Receiving Data value turns green when the Source, Destination, or Device IP field of an event matches the IP address of the asset. Gray means that no data is being received.

Set up Log Management

Plugin(s) successfully configured. Configure each asset to send logs by clicking on the instructions provided. Once the asset is configured AlienVault should detect the incoming data. When AlienVault receives data for a asset the "Receiving Data" light will turn green. Click "Finish" when you have received data from at least one asset.

ASSET	TYPE	PLUGIN ENABLED	RECEIVING DATA	INSTRUCTIONS
Host-192-168-73-2 (192.168.73.2)	Cisco ASA Adaptive Security Appliance			Instruction to forward logs
Host-192-168-73-2 (192.168.73.2)	Citrix NetScaler			Instruction to forward logs

- To learn how to configure your assets to send data to USM Appliance, click **Instructions to forward logs**.

After you have enabled plugins for your assets, click **Next** at the bottom-right corner to proceed.

Connecting to AlienVault Open Threat Exchange®

AlienVault Open Threat Exchange® (OTX™) is an open information sharing and analysis network, created to put effective security measures within the reach of all organizations. Unlike invitation-only threat sharing networks, OTX provides real-time, actionable information to all who want to participate.

Enabling AlienVault OTX in your installation will allow you to automatically share anonymous threat information with the OTX community. In return you will receive crowd-sourced threat updates every 30 minutes. The image below shows a sample of the data being sent from an AlienVault USM Appliance installation to OTX.

The following data are collected

- The source and/or destination IP address of an event.
- The name of the event.
- The number of times such event occurred.

DESTINATION ALL:			SOURCE ALL:		
HOST	EVENT	COUNT	HOST	EVENT	COUNT
216.151.164.5	snort: "ET TROJAN Possible Graftor EXE Download Common Header Order"	4	216.151.164.5	snort: "ET CURRENT_EVENTS Malicious Redirect 8x8 script tag"	1
216.151.164.5	directive_event: AV Malware, malware infection detected on SRC_IP	1	216.151.164.5	directive_event: AV Client side attack, external host delivered known exploit kit component and executable, successful exploitation to DST_IP	1
216.151.164.5	directive_event: AV Malware, trojan connecting to a low reputation CnC server on SRC_IP	2	216.151.164.5	directive_event: AV Misc, suspicious executable download from a bad IP reputation web site on DST_IP	2

After you finish installing and configuring AlienVault USM Appliance (with OTX enabled), you will be able to quickly see which alarms indicate malicious activity from a known bad actor on the Alarms page. For more information, see [Using OTX in USM Appliance](#).

To enable OTX in your USM Appliance installation, you must enter the OTX key and connect to your OTX account. If you do not have an OTX account and would like to sign up for it, you can do so from the Getting Started Wizard.

To join OTX from the Getting Started Wizard

1. On the Join OTX screen, click **Sign Up Now**.

A popup takes you to the sign-up page on <https://otx.alienvault.com/accounts/signup/>.

2. Fill out the information (username, email address, and password) and click **Sign Up**.

A page appears informing you that a verification email with a link to OTX was sent to the email address you provided.

3. After you receive the email, click the link and, on the confirmation page for logged-in USM Appliance users, click **Login**.

A USM Appliance key page appears, displaying your OTX key and stating that the username you used to register for OTX is logged in.

4. Copy the OTX key and paste it into the **Enter OTX Key** field shown in the following illustration.
5. Click **Next**.

The Thank You for Joining the Open Threat Exchange page appears.

6. Click **Finish**.

Join the Open Threat Exchange - Threat Intelligence for You, Powered by the Community

What is OTX?

AlienVault Open Threat Exchange (OTX™) is the world's first truly open threat intelligence community. OTX enables all participants to strengthen their network security defenses with community-powered, accurate, relevant, and confirmed threat intelligence. OTX also allows everyone to collaborate by actively discussing and sharing the latest threat data and research, strengthening their own defenses while helping others do the same.

Why should I join?

With AlienVault OTX, you can respond faster to changes in the threat landscape by receiving real-time, detailed, community-powered threat intelligence. OTX enables you to automatically instrument your USM and OSSIM deployments with the latest actionable threat intelligence from community-generated "Pulses". Pulses provide specific, actionable information including Indicators of Compromise (IoCs) that help you to detect the latest threats.

How does it work?

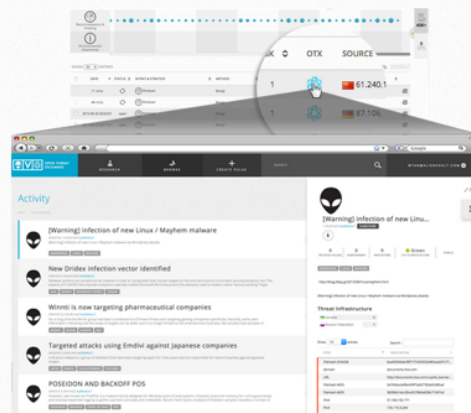
Enabling OTX in your USM installation will enable you integrate OTX Pulses containing the latest threat intelligence, including Indicators of Compromise (IoC) into your installation. These pulses will be used in correlation on security events to provide you with deeper insight into the activities happening on your network. Additionally, you can contribute to the community by sending anonymous threat data to OTX. [See what data is being sent to OTX.](#)

To enable OTX in your installation, sign up for an OTX Account. You will receive an OTX key to connect to your installation.

SIGN UP NOW

Enter your OTX key below to connect your account.

Enter OTX key



Important: After you click Finish, you cannot run the Getting Started Wizard again.

IDS Configuration

Topics covered in this section include

Intrusion Detection Systems	122
AlienVault HIDS	124
AlienVault NIDS	163

Intrusion Detection Systems

An Intrusion detection system (IDS) monitors networks and hosts in searching for malicious activities or policy violations, such as compromise of confidentiality, of system security, or of integrity. Some IDS systems may be capable of stopping an intrusion attempt but this is neither required nor expected of an IDS system. IDS systems primarily focus on identifying possible intrusions, logging information about them, and reporting attempts, which security analysts can further analyze.

Classic network firewalls analyze network and transport layer headers, such as source and destination IP address, protocol, and source and destination ports. However, attackers today do not only aim at network and transport layers any more, since network firewalls protect them well; instead, they focus on exploiting vulnerabilities in operating systems, applications, and protocols. Network firewalls cannot detect such attacks. Therefore, you need additional security systems, such as IDS, in order to detect them. Other examples of attacks that IDS can detect but firewall cannot include:

- Attacks that use tunneling, also known as "port forwarding", inside legitimate traffic or encryption
- Attacks within internal networks

IDS systems generally fall into two categories:

- Network IDS (NIDS)—Placed at strategic points in a network to monitors traffic between devices and hosts within the network.
- Host-Based IDS (HIDS)—Runs on individual host systems and monitors traffic from and to the host system as well as activities on the system itself.

USM Appliance provides both network and host-based intrusion detection capabilities.

Network Intrusion Detection System (NIDS)

You typically place a Network Intrusion Detection System (NIDS) on the inside of a network firewall, where it can monitor traffic from and to all devices. This way, the NIDS detects malicious activities that fall through the network firewall. A NIDS usually works in promiscuous mode, by monitoring a copy of the network traffic. It analyzes the traffic by comparing it against a database of known attacks, also known as signatures, or by detecting anomalies in traffic patterns. When identified, a NIDS event is generated and reported to the management station.

You can use the following devices to forward network traffic to a NIDS:

- Network hubs
- Network switches with mirrored or spanned ports

Advantages of NIDS:

- It monitors the entire network's traffic if placed correctly in a network.
- It has no impact on network performance and throughput since it only analyzes the copy of the network traffic.
- It has no impact on network availability since it does not stand inline with network traffic.

Limitations of NIDS:

- It cannot analyze encrypted information.
- It requires continued signature updates.
- It requires specific network configuration to receive a copy of the traffic.
- It cannot block the attacks.

Host Intrusion Detection System (HIDS)

A Host-base Intrusion Detection System (HIDS) monitors the behavior and state of a computer system, as well as network packets that the system sends and receives. A HIDS runs as an agent on a system, which sends detected events to a management station. The HIDS agent usually monitors which programs access which resources and determines if an application made an unauthorized change in memory, a file, or a database. A HIDS can also look at the state of a system and monitor system-specific logs in order to detect any significant changes on the system.

While a NIDS detects attacks sent over a network that the NIDS monitors, a HIDS detects those against the hosts on the network. NIDS cannot detect events in packet flows that use encryption, but HIDS can after the host decrypts the traffic. Ideally, a HIDS should work side-by-side with a NIDS. You can correlate events detected by both systems to determine if an attack was successful. For example, a detected network attack followed by the creation of an administrator account on a server could mean that the attack was successful.

Advantages of HIDS:

- It can detect if an attack was successful or not.
- It monitors system activities.
- It can detect changes in files, memory, and applications.
- It can detect attacks that NIDS fails to detect, such as changes from a system console.

Limitations of HIDS:

- You need to deploy an agent to each host you want to monitor.
- It does not detect network scans or reconnaissance attacks.
- The host it resides on is susceptible to attack and disablement.

AlienVault HIDS

This section covers the following subtopics:

- [AlienVault HIDS](#)
- [Deploy AlienVault HIDS Agents](#)
- [File Integrity Monitoring](#)
- [Agentless Monitoring](#)
- [Working with AlienVault HIDS Rules](#)
- [Tutorial: Reading a Log File with a HIDS Agent on Windows](#)

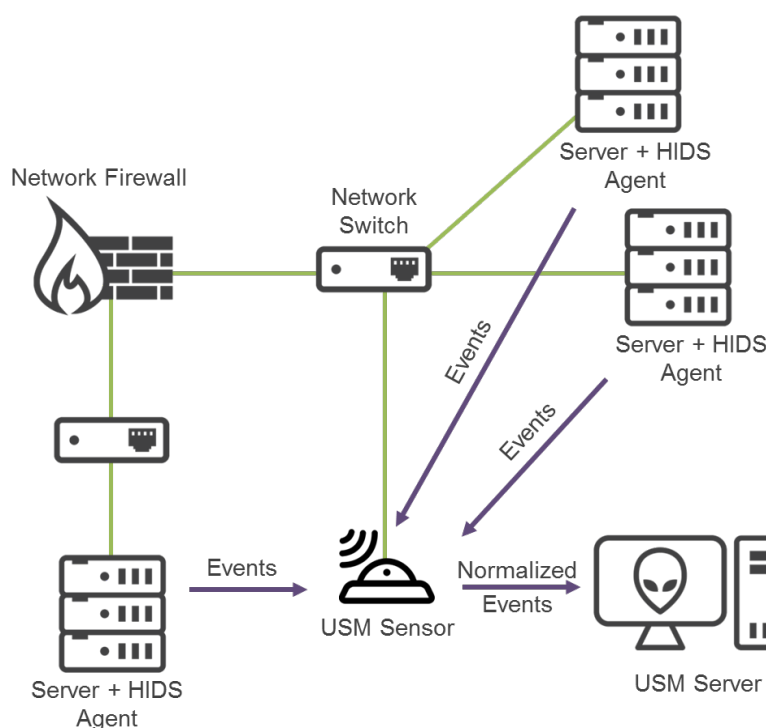
AlienVault HIDS

The AlienVault HIDS included in the USM Appliance provides the following features:

- Log monitoring and collection
- Rootkit detection
- File integrity monitoring
- Windows registry integrity monitoring
- Active response that can run applications on a server in response to certain triggers, such as specific alerts or alert levels

AlienVault HIDS uses a server/agent architecture, where the HIDS agent resides on hosts you want to monitor; and the HIDS server resides on the USM Appliance Sensor. The USM Appliance Sensor receives events from the HIDS agents, normalizes them, and sends them to the USM Appliance Server for analysis, correlation, and storage. AlienVault HIDS also has some limited support for agentless operation on Linux for log retrieval only.

You need to deploy the HIDS agents to client systems. The HIDS agent runs as a continuous in-memory service, interacting with the USM Appliance Sensor through UDP port 1514. The USM Appliance Sensor generates and distributes a pre-shared key to the HIDS agents, which then use the key to authenticate the communication between the HIDS agents and the USM Appliance Sensor.



AlienVault HIDS diagram

While HIDS agents are ideal for collecting Windows Security and System event logs, it is more effective to use NXLog to collect Application logs on Windows. AlienVault provides NXLog plugins for Microsoft IIS, Microsoft DHCP Server, Microsoft Exchange Server, and Microsoft SQL Server. For a complete list, see [NXLog Plugins](#).

Deploy AlienVault HIDS Agents

You can deploy an AlienVault HIDS agent to a host

- Through the Getting Started Wizard

This option supports deployment to Windows hosts and agentless deployment to Linux hosts. For instructions, see [Deploying HIDS to Servers](#), in the *Getting Started Wizard* topic.

- From the Asset List View

This option supports deployment to Microsoft Windows servers only. For instructions, see *Deploying HIDS Agents*, in *Asset Management*.

- From the HIDS management view

This option supports deployment to Windows and Linux hosts.

- [Deploy AlienVault HIDS Agents to Windows Hosts](#)
- [Deploy the AlienVault HIDS Agents to Linux Hosts](#)
- [Deployment Verification](#)
- [Appendix: AlienVault HIDS Agent Deployment Status Messages](#)

Deploy AlienVault HIDS Agents to Windows Hosts

For Microsoft Windows hosts, USM Appliance generates a binary file containing the appropriate server configuration and authentication key. You can choose to let USM Appliance install the file for you, or download the file and install it on the host yourself.

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 whitelist. 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 NTLMSPPP 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

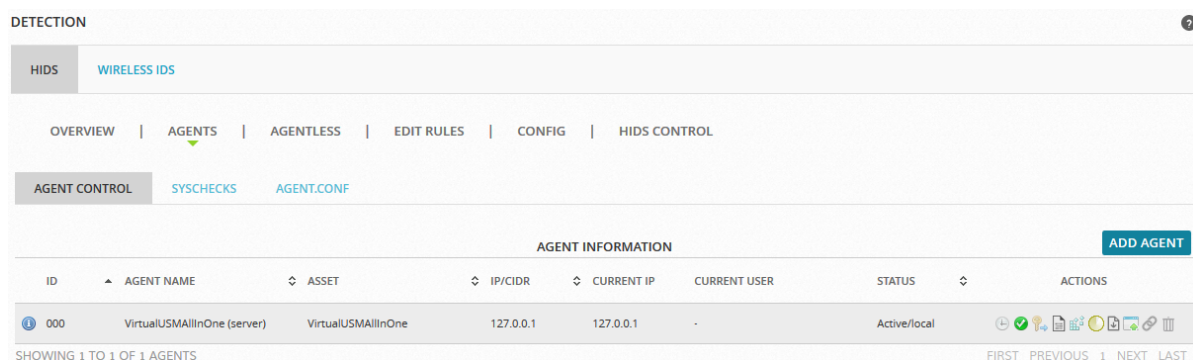
1. Go to **Control Panel > Folder Options > View**.
2. Deselect **Use Sharing Wizard (Recommended)**.
3. Go to **Control Panel > System and Security > Windows Firewall > Advanced Settings > Inbound Rules**.
4. Enable **File and Printer Sharing (SMB-In)**.
5. Enable **Windows Management Instrumentation (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 whitelist the IP address of USM Appliance, or temporarily disable the antivirus software during the installation.

To deploy the AlienVault HIDS agent to a Windows host

1. Go to **Environment > Detection**.
2. Go to **HIDS > Agents > Agent Control > Add Agent**.



3. On New HIDS Agent, select the host from the asset tree.

USM Appliance populates **Agent Name** with the host name, and **IP/CIDR** with the host IP address automatically.


4. Click **Save**.

USM Appliance adds the new agent to the list.

5. To deploy the agent, click the  button in the Actions column.

6. In Automatic Deployment for Windows, type the **Domain** (optional), **User**, and **Password** of the host; then click **Save**.

USM Appliance assembles a preconfigured binary file and deploys it to the host.

7. Alternatively, to download the preconfigured binary file, click the  button in the Actions column.

Your browser downloads the file automatically or prompts you for the download.

8. Transfer the file, named `ossec_installer_<agent_id>.exe`, to the Microsoft Windows host.

9. On the Windows host, double-click to run the executable.

The installer runs in a console briefly, then displays a progress bar until completion.

Deploy the AlienVault HIDS Agents to Linux Hosts



Important: For Linux hosts, depending on which distribution of Linux you use, AT&T Cybersecurity recommends that you download the corresponding `ossec-hids-agent` installer file from the [OSSEC's Downloads page](#) directly, and then follow their instructions to complete the installation.

After you have successfully installed the HIDS agent on the Linux host, perform the steps below to connect it to USM Appliance.


To add the HIDS agent to USM Appliance

1. Go to **Environment > Detection**.
2. Go to **HIDS > Agents > Agent Control > Add Agent**.
3. On New HIDS Agent, select the host from the asset tree.

USM Appliance populates **Agent Name** with the host name, and **IP/CIDR** with the host IP address automatically.

4. Click **Save**.

USM Appliance adds the new agent to the list.

5. To extract the key for the agent, click the  button in the Actions column, and then copy the key that displays.

Search

AGENT INFORMATION

ADD AGENT

ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
<div><div></div><div>000</div></div>	VirtualUSMAllinOne (server)	VirtualUSMAllinOne	127.0.0.1	127.0.0.1	-	Active/focal	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
<div><div></div><div>001</div></div>	Host-10-47-30-101	Host-10-47-30-101	10.47.30.101	-	-	Disconnected	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>

SHOWING 1 TO 2 OF 2 AGENTS

FIRSTPREVIOUS1NEXTLAST

Agent key information for '001' is:
MDAxIEhvc3QlMTAINDctMzAMTAxIDEwLjQ3LjMwLjEwMSA1NTZhMTc2YWQ3MDE5ODY1NTQ0MjIwYjE5ZDAzMWE0ZWVhYTYSY2VlNTVjYjk2NjkyOTIzNjBzRlMmFmOTli

6. Login to the Linux host, run `/var/ossec/bin/manage_agents`, and then enter `I` to import the key you copied in the previous step.



Note: On some installations, Centos, for example, the command may be `manage_client` instead of `manage_agents`.

7. Edit `/var/ossec/etc/ossec-agent.conf` to change the server IP address to the USM Appliance.

8. Start the HIDS agent if it is not already running:

```
service ossec start
chkconfig ossec-hids on
```

9. On the USM Appliance, go to **Environment > Detection**, click **HIDS Control**, and then **Restart**.

Deployment Verification

You can verify the deployment both on the HIDS agent and in USM Appliance.

On the HIDS agents, you can check the `ossec.log` file to make sure that a message similar to the following exists:

```
2015/09/18 09:07:38 ossec-agent: INFO: Started (pid: 3440).
2015/09/18 09:07:38 ossec-agent(4102): INFO: Connected to the server
(10.47.30.100:1514).
```

To check the agent log file on the Windows hosts

1. Go to **Start > OSSEC > Manage Agent**.
2. In OSSEC Agent Manager, click **View** and select **View Logs**.

This opens the `ossec.log` file on the agent.

To check the agent log file on the Linux hosts

1. Login to the Linux host.
2. In a console, enter the following:

```
more /var/ossec/logs/ossec.log
```

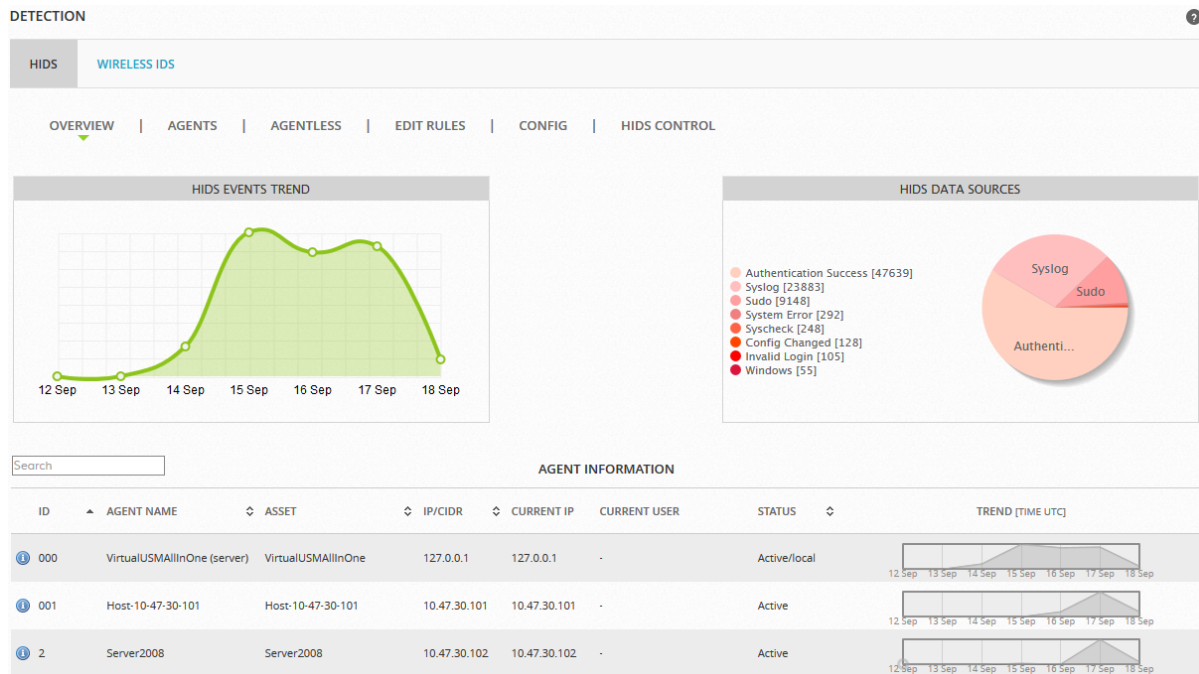
On the USM Appliance, make sure there are AlienVault HIDS events.

To verify the HIDS deployment in USM Appliance

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

The Overview page for HIDS displays.

2. Ensure that the Status column for the deployed agents display **Active**, and the Trend chart is not empty.



- To see the AlienVault HIDS events from a specific agent, go to **Analysis > Security Events (SIEM)**.
- In **Data Sources**, select AlienVault HIDS; change **Event Name** to Src IP, enter the IP addresses of the HIDS agent, and then click **Go**.

The AlienVault HIDS events from the particular agent display.

By default, USM Appliance updates the HIDS Agent information in its database every 60 minutes. If you want to increase the frequency, you can change the refresh rate under Configuration > Administration > Main > Detection.

Appendix: AlienVault HIDS Agent Deployment Status Messages

You may see the following messages in the web UI when deploying AlienVault HIDS agents in USM Appliance.

USM Appliance HIDS agent deployment status messages

Message	Explanation
Agent ID '<agent_id>' is not valid. Agent ID has to be 1-4 digital characters.	The HIDS agent ID provided is not valid.
Cannot create HIDS agent '<agent_name>' on the sensor '<sensor_id>'.	The HIDS agent cannot be added to the given sensor.

USM Appliance HIDS agent deployment status messages (Continued)

Message	Explanation
Cannot get HIDS agents related to asset <asset_id>.	The HIDS agent information cannot be retrieved.
Cannot resolve the given asset <asset_id>.	The asset ID is not a valid UUID.
Cannot resolve the given sensor <sensor_id>.	The sensor ID is not found in the database.
Deployment IP '<ip_address>' is not valid IP address.	The IP address provided is not a valid IP address.
HIDS Agent cannot be deployed. Reason: <error_msg>.	The errors received from the commands used to deploy the HIDS agent in the target host.
HIDS agent successfully deployed.	The HIDS agent deployment is successful.
Invalid Credentials: '<username>' is not valid username.	The username contains characters that are not allowed.
Invalid Credentials: Password is not valid.	The password contains characters that are not allowed.
Sorry, deployment job cannot be launched due to an error when sending the request. Please try again.	The job to deploy the HIDS agent cannot be launched.

File Integrity Monitoring

You can configure AlienVault HIDS to perform File Integrity Monitoring (FIM), which identifies changes in system files, folders, and Microsoft Windows registries. The process that identifies these changes is *syscheck*. The *syscheck* process scans the host at user-defined intervals and stores checksums of watched files. The system then generates an event when a checksum changes.

In addition to using *syscheck*, you can also configure Windows systems so that AlienVault HIDS agents forward object access audit events for USM Appliance to process. These events provide more information on operations affecting file and folder objects, such as who performed specific actions or operations on an object. For more information, see [Configuring Windows Systems to View Windows Audit Object Access Events](#).

Configuring File Integrity Monitoring

Every HIDS agent includes an `ossec.conf` file with some default settings for syscheck. On Microsoft Windows hosts, you can find this file in `C:\Program Files (x86)\ossec-agent`, and on Linux, in `/var/ossec/etc`.

When you make changes through the USM Appliance web interface, USM Appliance records your modifications in the `agent.conf` file and stores it for distribution. When the agent authenticates, it will download the shared configuration and merge it with the local copy. The shared file will take precedence, overwriting any local configuration.

Default settings for the `ossec.conf` file stored on a host system are configured when the HIDS agent is first installed or deployed on a host system. In addition, an `ossec.conf` file containing syscheck and other global options is defined and stored on the USM Appliance Server. For more information on viewing and configuring this file, see [To configure USM Appliance server-side \(global\) ossec.conf settings](#).

To change syscheck options for all agents

1. Go to **Environment > Detection**.
2. On HIDS, click **Agents**, and then click **Syschecks**.
3. Configure the options according to your needs.
4. Click **Save** after making changes in each section.
5. (Optional) Click **Agent.conf** to confirm the changes in XML format.
6. To apply your changes immediately, click **HIDS Control**, and then **Restart**.

To configure USM Appliance server-side (global) ossec.conf settings

1. Go to **Environment > Detection**.
2. On HIDS, click **Config**, and then click **Syschecks**.
3. Configure the options according to your needs.
4. You can also view the contents of the server `ossec.conf` file in XML format by selecting the **Config > Configuration** option.

The following table describes syscheck options that you can specify through the USM Appliance web interface.

Syscheck options

Options		Meanings	Default Values
Frequency		Frequency at which the syscheck executes (in seconds).	72000s (20h)
Scan_day		Day of the week to run the scans.	None
Alert New Files		Whether to alert on new files created. (Global agent option; not configurable for individual hosts.)	No
Scan Time		Time to start the scans.	None
Auto Ignore		Whether to ignore files that change too often. (Global agent option; not configurable for individual hosts.)	No
Scan on Start		Whether to do the first scan as soon as the agent starts.	Yes
Windows Registry Entries Monitored		Microsoft Windows registries to monitor.	See the <code>ossec.conf</code> file on a Windows host
Registry Entries Ignored		Microsoft Windows registries not to monitor.	See the <code>ossec.conf</code> file on a Windows host
Files/Directories Monitored		Files or directories to monitor.	See the <code>ossec.conf</code> file on a Windows host
	Realtime	Real time or continuous monitoring on Linux (using the <code>inotify</code> system calls) and Windows systems.	No
	Report Changes	(Linux-like systems only) Whether to report file changes. Limited to text files.	No
	Chk All	Checks all changes listed below.	No
	Chk Sum	Check the md5 and sha1 hashes of the files.	No
	Chk Sha1sum	Check the sha1 hashes of the files.	No
	Chk Size	Checks the size of the files.	No
	Chk Owner	Checks the owner of the files.	No

Syscheck options (Continued)

Options		Meanings	Default Values
	Chk Group	Checks the group owner of the files/directories.	No
	Chk Perm	Checks the permission of the files/directories.	No
File/Directories Ignored		Files or directories not to monitor.	See the <code>ossec.conf</code> file on a Windows host

About Auto Ignore and Realtime

With Auto Ignore set to `No`, you receive alerts on every file change, regardless how many times it is changed. If you also select the Realtime option, the alert stops after the third change, equivalent to setting Auto Ignore to `Yes`.

About Alert New Files

You can configure AlienVault HIDS to alert on new files, but it does not report in real time, because AlienVault HIDS can only detect new files on a full scan.

To enable alerting on new files

1. Change **Alert New Files** to `Yes`.
2. Specify the directory in which to detect the new files.
3. Select **Chk All**.

About Report Changes

The `report_changes` option is only available on UNIX-like systems. Setting this option globally, or reporting on changes to the root file system, will likely create a large number of events, which could potentially fill up all available disk space and impact USM Appliance operation.

Specifying Different Syscheck Options for Different Hosts

You can configure different syscheck options for different hosts, by entering them in the `agent.conf` file manually. Ensure that you

- Use a separate `<agent_config>` element for each host you need to configure.
- Use the `name` attribute to denote the name of the host. (This is the agent name used when adding the agent to the detection section.)

- Specify the options you want to change inside the `<syscheck>` element.
- Repeat all every host you want to configure.

The following example shows different syscheck options for host AD2012 and Win2008:

```
<agent_config name="AD2012">
<syscheck>
<frequency>21600</frequency>
<scan_on_start>yes</scan_on_start>
<directories check_all="yes">C:\temp</directories>
</syscheck>
</agent_config>

<agent_config name="Win2008">
<syscheck>
<frequency>3600</frequency>
<scan_on_start>yes</scan_on_start>
<directories check_all="yes">C:\topsecret</directories>
</syscheck>
</agent_config>
```

Instead of making these changes on the hosts one-by-one, you can configure them in the USM Appliance web interface.

To configure different syscheck options for different hosts

1. Go to **Environment > Detection**.
2. On HIDS, click **Agents > Agent.conf**.

By default, this page is blank.
3. Type or paste in the changes you want to make.
4. Click **Save**.
5. (Optional) Click **Syscheck**. Notice that a list appears towards the upper-right corner with

the name of the first entry in `agent.conf`.

HIDS WIRELESS IDS

OVERVIEW | AGENTS | AGENTLESS | EDIT RULES | CONFIG | HIDS CONTROL

AGENT CONTROL | SYSCHECKS | AGENT.CONF

Select agent config block: **name = "AD2012"**

CONFIGURATION PARAMETERS

FREQUENCY	21600	SCAN TIME	:
SCAN_DAY	-- Select a day --	SCAN ON START	Yes

SAVE

WINDOWS REGISTRY ENTRIES MONITORED (WINDOWS SYSTEM ONLY)

WINDOWS REGISTRY ENTRY

ACTIONS

SAVE

REGISTRY ENTRIES IGNORED

REGISTRY ENTRY IGNORED

ACTIONS

SAVE

FILES/DIRECTORIES MONITORED

FILES/DIRECTORIES	REALTIME	REPORT CHANGES	CHK ALL	CHK SUM	CHK SHA1 SUM	CHK SIZE	CHK OWNER	CHK GROUP	CHK PERM	ACTIONS
C:\temp	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

SAVE

- To apply your changes immediately, click **HIDS Control**, and then **Restart**.

Viewing the File Integrity Monitoring Events

Each time an AlienVault HIDS agent detects a change in a monitored file or directory, USM Appliance creates an event and stores it in the database.

To view FIM events

- Go to **Analysis > Security Events (SIEM)**.
- In **Data Sources**, select "AlienVault HIDS".
- In **Event Name**, type "Integrity".
- Click **Go**.

SECURITY EVENTS (SIEM)

SIEM REAL-TIME EXTERNAL DATABASES

Search for "Integrity"

SHOW EVENTS

DATA SOURCES: AlienVault HIDS

DATA SOURCE GROUPS:

SENSORS: ☐ EXCLUDE

ASSET GROUPS:

NETWORK GROUPS:

RISK:

OTX IP REPUTATION:

OTX PULSE:

☐ ONLY OTX PULSE ACTIVITY

userdata1

Advanced Search:

EVENTS GROUPED TIMELINE

GROUP EVENTS BY:

DISPLAYING 1 TO 3 OF 3 EVENTS. 19,758 TOTAL EVENTS IN DATABASE.

EVENT NAME	EVENTS # (*)	UNIQUE SRC. #	UNIQUE DST. #	LATEST EVENT	GRAPH
<input type="checkbox"/> AlienVault HIDS: Integrity checksum changed.	22	1	1	2016-10-26 13H	
<input type="checkbox"/> AlienVault HIDS: Integrity checksum changed again (2nd time).	11	1	1	2016-10-26 06H	
<input type="checkbox"/> AlienVault HIDS: Integrity checksum changed again (3rd time).	1	1	1	2016-10-26 13H	

5. View event details to determine which file has changed.

EVENT DETAILS

Hostname: Server2008
MAC Address: 00:50:56:02:68:68
Port: 0
Latest update: N/A
Username & Domain: N/A
Asset Value: 4

Location: N/A
Context: N/A
Asset Groups: [Headquarters Assets, Critical Assets](#)
Networks: [LabNetwork](#)
Logged Users: N/A
OTX IP Reputation: No

SERVICE PORT PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST

Hostname: Server2008
MAC Address: 00:50:56:02:68:68
Port: 0
Latest update: N/A
Username & Domain: N/A
Asset Value: 4

Location: N/A
Context: N/A
Asset Groups: [Headquarters Assets, Critical Assets](#)
Networks: [LabNetwork](#)
Logged Users: N/A
OTX IP Reputation: No

SERVICE PORT PROTOCOL

No services available

SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST

File that has been changed

RAW LOG

```
AV - Alert - "143439326" --> RID: "550"; RL: "7"; RG: "ossec,syscheck"; RC: "Integrity checksum changed."; USER: "None"; SRCIP: "None";
HOSTNAME: "Server2008" 10.47.30.102->syscheck; LOCATION: "(Server2008) 10.47.30.102->syscheck"; EVENT: "([INIT])Integrity checksum changed for:
'c:\Users\fd\text\Nsize changed from '54' to '226'\nOld md5sum was: '286a68da218999912453b44ed70c17'\nNew md5sum is :
'0fd51614a63e59976dcf67b0dd560de81'\nOld sha1sum was: '1e4dfd33d4e1d23b2f4a9c4f9f33260579b5f6a3'\nNew sha1sum is :
'28ba3523e7c365b8f808cc8671ceb41ae13132f3'\n[END]";
```

Configuring Windows Systems to View Windows Audit Object Access Events

To configure Windows systems so that AlienVault USM Appliance can view Windows audit object access events, you need to first edit local security policy settings. After applying policy changes to include audit object events in Windows security logs, the AlienVault HIDS agent will forward those events to USM Appliance.

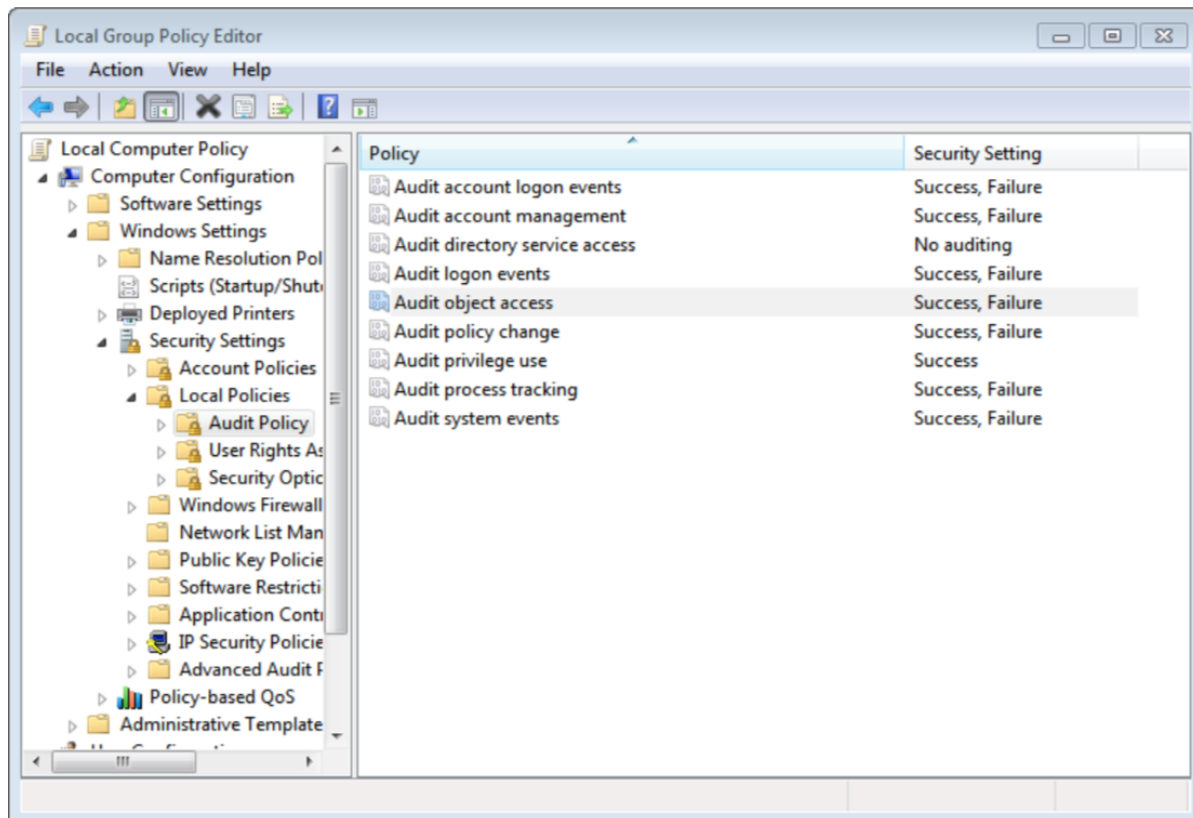


Note: You can only set up file and folder auditing on NTFS drives.

To define policy settings for object access audit events

1. On a selected Windows system, open the **Local Group Policy Editor**.
2. Go to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy**.
3. Edit the **Audit object access** policy and enable auditing of **Success** and **Failure** attempts.

The following display shows an example:



To apply or modify auditing policy settings

1. Open **Windows Explorer** and navigate to the file or folder you want to audit.
2. Right-click on the file or folder and select **Properties**.
3. Select the **Security** tab and click **Advanced**.
4. Select the **Auditing** tab and click **Continue** if prompted.
5. Perform one of the following operations:

- To set up auditing for a new user or group, click **Add**. In the **Enter the object name to select** field, type the name of the user or group that you want to audit, then click **OK**.
 - To remove auditing for an existing group or user, highlight the group or user name, click **Remove**, and then click **OK**. You can skip remaining steps.
 - To view or change auditing for an existing group or user, click its name and then click **Edit**.
6. In the **Apply onto** box, click the location that you want to audit.
 7. In the **Access** box, indicate what actions you want to audit by selecting the appropriate check boxes.
 8. If you want to prevent subordinate files and subfolders of the original object from inheriting audit settings, select the **Apply these auditing entries to objects and/or containers within this container only** check box.



Note: Because the Windows security log is limited in size, select the files and folders to be audited carefully, since new audit events will be stored there. Also, consider the amount of disk space that you want to devote to the security log. The maximum size for the security log is set in Event Viewer.

After enabling object access auditing, you can view the security log in Event Viewer to see that the audit events are now collected. The AlienVault HIDS agent will forward those events to USM Appliance.

USB Device Monitoring on Windows Systems

In AlienVault USM Appliance version 5.3, Host Intrusion Detection System (HIDS) rules and plugins have been updated to capture USB device events on Windows machines.

Configuration Changes on the HIDS Agent

If you are deploying USM Appliance version 5.3 or later, you do not need to do anything. This feature is enabled by default.

If you are updating to USM Appliance version 5.3 or later from a previous version, and you want to use the USB device detection feature, you need to do one of the following:

- On the host you wish to monitor, remove the existing HIDS agent and redeploy it. For instructions, see [Deploy AlienVault HIDS Agents to Windows Hosts](#).
- Alternatively, you can change the configuration on Windows manually, as detailed below.

Change the Configuration on Windows Manually

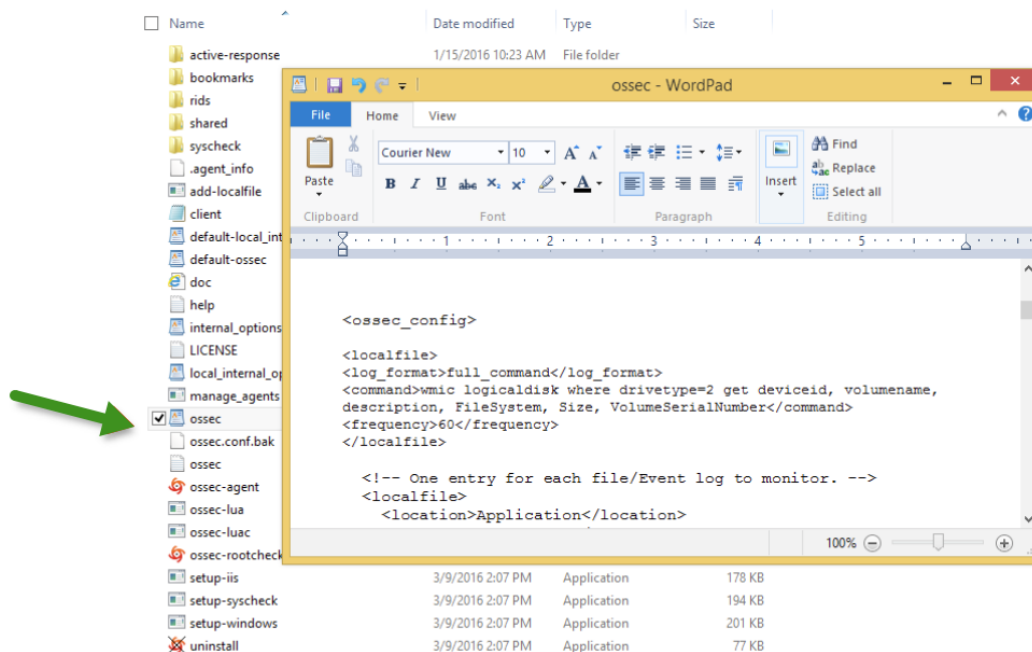
Since `full_command` must be configured in each Windows system's `ossec.conf` file, you need to change the HIDS agent configuration on each Windows machine that you want to monitor USB devices.

To change the configuration on the client machine:

1. Go to `C:\Program Files (x86)\ossec-agent`.
2. Open `ossec.conf` with a text editor.
3. Locate the line "`<ossec_config>`" and add the following configuration right below that line:

```
<localfile>
<log_format>full_command</log_format>
<command>wmic logicaldisk where drivetype=2 get deviceid, description,
FileSystem, Size, VolumeSerialNumber</command>
<frequency>60</frequency>
</localfile>
```

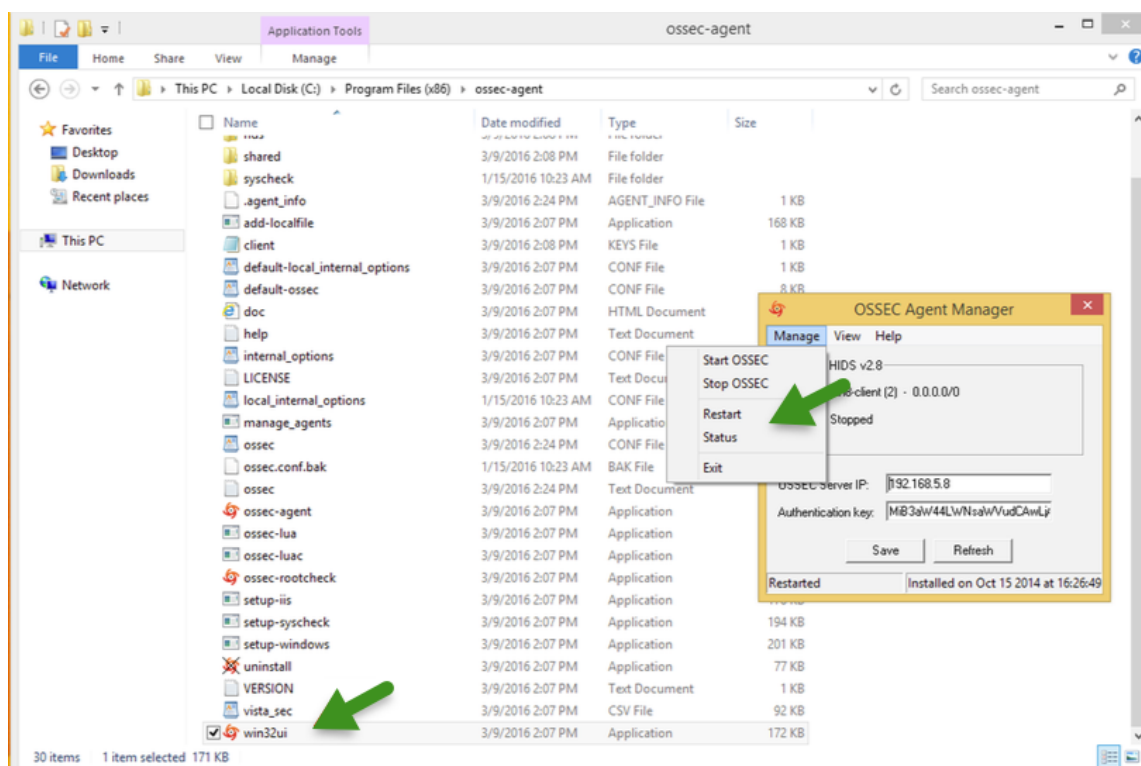
Your configuration file should look similar to this:



Some customers have reported that the `wmic` command above does not work in their environment. AlienVault has not been able to reproduce the problem but suspect that it may be related to newer HIDS versions or older Windows versions. If you run into the same issue, try using the following command instead:

```
<command>wmic logicaldisk where "drivetype=2 AND NOT deviceid like 'a\\'"
get deviceid, description, FileSystem, Size, VolumeSerialNumber</command>
```

4. Launch the `win32ui` application located in the same directory.
 - a. Select **Manage**.
 - b. Click **Restart**.



Verification

Once USB activity has been detected on that host, you should be able to see new AlienVault HIDS events with the event name **AlienVault HIDS: New USB Device Found**. And the Event Details pane includes information about Drive, FileSystem, Size, and Serial Number:

DATE	2016-09-09 16:15:01 GMT-4:00	CATEGORY	System
ALIENVAULT SENSOR	1752-16-10000000	SUB-CATEGORY	Notification
DEVICE IP	1752-16-10000000	DATA SOURCE NAME	AlienVault HIDS-windows
EVENT TYPE ID	100051	DATA SOURCE ID	7006
UNIQUE EVENT ID#	76ca11e6-a576-000c-2989-a95d1b1be754	PRODUCT TYPE	Operating System
PROTOCOL	TCP	ADDITIONAL INFO	N/A

PRIORITY	RELIABILITY	RISK	OTX INDICATORS
2	2	LOW (0)	0

SOURCE		DESTINATION	
Hostname: N/A	Location: N/A	Hostname: N/A	Location: N/A
MAC Address: N/A	Context: N/A	MAC Address: N/A	Context: N/A
Port: 0	Asset Groups: N/A	Port: 0	Asset Groups: N/A
Latest update: N/A	Networks: N/A	Latest update: N/A	Networks: N/A
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

SERVICE	▲	PORT	◆	PROTOCOL	◆
No services available					
SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST					

SERVICE	▲	PORT	◆	PROTOCOL	◆
No services available					
SHOWING 0 TO 0 OF 0 SERVICES FIRST PREVIOUS NEXT LAST					

USERNAME
None

RAW LOG
AV - Alert - "1473452101" --> RID: "100051"; RL: "7"; RG: "USB Detection,"; RC: "New USB Device Found." USER: "None"; SRCIP: "None"; HOSTNAME: "1752-16-10000000"; -->wmic logicaldisk where "drivetype=2 AND NOT deviceid like 'a\\'" get deviceid, volumename, description, FileSystem, Size, VolumeSerialNumber"; LOCATION: "1752-16-10000000"; -->wmic logicaldisk where "drivetype=2 AND NOT deviceid like 'a\\'" get deviceid, volumename, description, FileSystem, Size, VolumeSerialNumber"; EVENT: "[INIT]ossec: output: 'wmic logicaldisk where 'drivetype=2 AND NOT deviceid like 'a\\'" get deviceid, volumename, description, FileSystem, Size, VolumeSerialNumber';\n\n[END]";

Agentless Monitoring

AlienVault HIDS allows you to run integrity checking without agents installed on hosts, network devices, routers, firewalls, or switches. Agentless monitoring detects checksum changes in files or runs diffs to shows what exactly has changed.

Prerequisites

Before enabling agentless monitoring, make sure you have done the following:

- Open the `SSH` daemon on your device listening on TCP port 22.
- Set up firewall rules to allow `SSH` traffic between USM Appliance and your device.

AlienVault HIDS runs checks periodically, communicating with monitored devices through TCP port 22 using the `SSH` protocol.

Enabling Agenless Monitoring

To enable agentless monitoring

1. Go to **Environment > Detection > Agentless**.
2. To add a new host you want to monitor, click **New** towards the right.
3. Fill out the **Agentless Data Configuration** information on the left.
4. Fill out the **Monitoring Entries Options** information on the right, then click **Add**.

Monitoring entries options

Fields	Values	Explanation	Supported Arguments by Type
Type	Integrity Check BSD	Performs BSD-specific integrity checking on folders.	List of folders to monitor. For example: <ul style="list-style-type: none"> • /bin • /etc/sbin
	Integrity Check Linux	Performs Linux-specific integrity checking on folders.	List of folders to monitor. For example: <ul style="list-style-type: none"> • /bin • /etc/sbin
	Generic Command Diff	Runs a list of commands you specify and creates an event if output changes.	List of commands whose output you want to compare. For example: <ul style="list-style-type: none"> • ls -la /etc • cat /etc/passwd
	Cisco Config Check	Checks device configuration using Cisco-compatible commands.	Leave it empty.
	Foundry Config Check	Checks device configuration using Foundry-compatible commands.	Leave it empty.
	ASA FWSMconfig Check	Checks device configuration using Cisco ASA-compatible commands.	Leave it empty.

Monitoring entries options (Continued)

Fields	Values	Explanation	Supported Arguments by Type
Frequency	(Default) 86400	How often AlienVault HIDS runs the checks, in seconds.	N/A
Arguments	/bin /etc/sbin	Arguments that correspond to the type of check you select. See the <i>Supported Arguments by Type</i> column in this table.	N/A



Important: USM Appliance can only process one argument for every entry. If you need to run multiple commands, put them in separate entries. The added entries appear in **Monitoring Entries Added**.

- Click **Update**.

DETECTION ?

HIDS WIRELESS IDS

OVERVIEW | AGENTS | AGENTLESS | EDIT RULES | CONFIG | HIDS CONTROL

←

Values marked with (*) are mandatory

AGENTLESS DATA CONFIGURATION		MONITORING ENTRIES OPTIONS	
HOSTNAME *	Linux	TYPE *	Integrity Check BSD
IP	10.47.30.101	FREQUENCY *	86400
SENSOR	VirtualUSMAllInOne	STATE	Periodic
SSH USERNAME *	root	ARGUMENTS	/bin /etc /sbin
SSH PASSWORD *	●●●●●●●●		
CONFIRM SSH PASSWORD *	●●●●●●●●		
(*) If you want to use public key authentication instead of passwords, you need to provide NOPASS as Normal Password			
PRIVILEGED PASSWORD			
CONFIRM PRIVILEGED PASSWORD			
(*) If you want to add support for 'su', you need to provide Privileged Password			
ENABLE USE_SU OPTION	<input type="checkbox"/>		
DESCRIPTION			

ADD

MONITORING ENTRIES ADDED				
TYPE	FREQUENCY	STATE	ARGUMENTS	ACTIONS
ssh_generic_diff	60	periodic_diff	ls /root	
ssh_integrity_check_linux	60	periodic	/bin /etc /sbin /root	

SHOWING 1 TO 2 OF 2 ENTRIES < PREVIOUS NEXT >

UPDATE

- To apply your changes immediately, click **HIDS Control**, and then **Restart**.

This starts the agentless service in the AlienVault HIDS.

Verifying the Agentless Deployment on USM Appliance

You can verify that you have successfully deployed the agentless monitoring in the following ways:

- On **Environment > Detection > Agentless**, the status of the host displays a green check mark and the **Agentless Status:** displays **Running**.

The screenshot shows the 'DETECTION' section of the AlienVault HIDS interface. The 'AGENTLESS' tab is selected, and the 'Agentless Status: Running' is highlighted in green. Below the status, a table lists the host details:

HOSTNAME	IP	USER	STATUS	DESCRIPTION
Linux	10.47.30.101	root	✓	

- On **Environment > Detection > HIDS Control**, make sure that you see "Agentless is running" in green.

The screenshot shows the 'HIDS CONTROL' section of the AlienVault HIDS interface. The 'HIDS CONTROL' tab is selected, and the 'Agentless is running' status is highlighted in green. Below the status, there are four action buttons: 'ENABLE', 'DISABLE', 'ENABLE', and 'STOP'. The 'HIDS OUTPUT' section shows the following log entries:

```

monitor is running...
logcollector is running...
remoted is running...
syscheckd is running...
analysed is running...
maild not running...
execd not running...
agentlessd is running...
  
```

- On **Environment > Detection > HIDS Control > HIDS Log**, make sure that you see the periodic checks performed.

DETECTION

HIDS WIRELESS IDS

OVERVIEW | AGENTS | AGENTLESS | EDIT RULES | CONFIG | HIDS CONTROL

HIDS CONTROL HIDS LOG ALERTS LOG

HIDS LOG View: 50

```

2015/09/18 06:28:14 remotel(4111): INFO: Maximum number of agents allowed: '2048'.
2015/09/18 06:28:14 remotel(1410): INFO: Reading authentication keys file.
2015/09/18 06:28:14 monitord: INFO: Started (pid: 17011).
2015/09/18 06:28:14 remotel: INFO: Assigning counter for agent Server2008: '0:2580'.
2015/09/18 06:28:14 remotel: INFO: Assigning sender counter: 0:453
2015/09/18 06:28:15 agentlessd: INFO: Test passed for 'ssh_integrity_check_linux'.
2015/09/18 06:28:18 syscheckd: INFO: Started (pid: 17007).
2015/09/18 06:28:18 rootcheckd: INFO: Started (pid: 17007).
2015/09/18 06:28:18 syscheckd: INFO: Monitoring directory: '/etc'.
2015/09/18 06:28:18 syscheckd: INFO: Monitoring directory: '/usr/bin'.
2015/09/18 06:28:18 syscheckd: INFO: Monitoring directory: '/usr/sbin'.
2015/09/18 06:28:18 syscheckd: INFO: Monitoring directory: '/bin'.
2015/09/18 06:28:18 syscheckd: INFO: Monitoring directory: '/sbin'.
2015/09/18 06:28:19 logcollector(1950): INFO: Analyzing file: '/var/log/messages'.
2015/09/18 06:28:19 logcollector(1950): INFO: Analyzing file: '/var/log/auth.log'.
2015/09/18 06:28:19 logcollector(1950): INFO: Analyzing file: '/var/log/syslog'.
2015/09/18 06:28:19 logcollector(1950): INFO: Analyzing file: '/var/log/mail.info'.
2015/09/18 06:28:19 logcollector(1950): INFO: Analyzing file: '/var/log/dpkg.log'.
2015/09/18 06:28:19 logcollector(1950): INFO: Analyzing file: '/var/log/apache2/error.log'.
2015/09/18 06:28:19 logcollector(1950): INFO: Analyzing file: '/var/log/apache2/access.log'.
2015/09/18 06:29:16 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Started.
2015/09/18 06:29:16 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Starting.
2015/09/18 06:29:20 syscheckd: INFO: Starting syscheck scan (pre-scan).
2015/09/18 06:29:30 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Finished.
2015/09/18 06:30:31 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Started.
2015/09/18 06:30:31 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Starting.
2015/09/18 06:30:46 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Finished.
2015/09/18 06:31:47 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Started.
2015/09/18 06:31:47 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Starting.
2015/09/18 06:31:47 agentlessd: INFO: ssh_integrity_check_linux: root@10.47.30.101: Starting.
    
```

- On **Analysis > Security Events (SIEM)**, make sure that you see events coming from the monitored host or device.

Filter for HIDS events

Advanced filter for source IP addresses

SIEM REAL-TIME EXTERNAL DATABASES

Search Signature ?

SHOW EVENTS

☐ Last Day
☐ Last Week
☐ Last Month
☒ Date Range
 2015-09-17 - 2015-09-17

DATA SOURCES

DATA SOURCE GROUPS

SENSORS ☐ EXCLUDE

ASSET GROUPS

NETWORK GROUPS

RISK

OTX IP REPUTATION

OTX PULSE

☐ ONLY OTX PULSE ACTIVITY

Advanced Search

Advanced Filter

AlienVault HIDS x

Date Range: time >= [09 / 17 / 2015] [03 : * : *] AND time [/ * / x] [any time]

Source=10.47.30.101 x

EVENTS GROUPED TIMELINE

SHOW TREND GRAPH ☐ Off

DISPLAYING 1 TO 16 OF 16 EVENTS. 164,313 TOTAL EVENTS IN DATABASE.

HIDS agentless events

<input type="checkbox"/>	SIGNATURE	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
<input checked="" type="checkbox"/>	AlienVault HIDS: Integrity checksum changed again (2nd time).	2015-09-18 06:46:07	VirtualUSMallInOne	N/A	Host-10-47-30-101	Host-10-47-30-101	0
<input checked="" type="checkbox"/>	AlienVault HIDS: Integrity checksum for agentless device changed.	2015-09-18 06:45:59	VirtualUSMallInOne	N/A	Host-10-47-30-101	Host-10-47-30-101	0
<input checked="" type="checkbox"/>	AlienVault HIDS: Integrity checksum changed.	2015-09-18 06:44:49	VirtualUSMallInOne	N/A	Host-10-47-30-101	Host-10-47-30-101	0

Working with AlienVault HIDS Rules

AlienVault HIDS expands from the open source project, OSSEC, by providing additional rules that are essential to identifying HIDS issues. The table below lists all the AlienVault-specific rules that USM Appliance provides out of the box.

AlienVault HIDS Rules

Rule File Name	Rules Purpose	Enabled by Default	Rule File Dependency	Windows Event ID Matched
alienvault-apache_rules.xml	Rules for Apache HTTP Server	No	apache_rules.xml	N/A
alienvault-directory-service_rules.xml	Detect changes of directory service objects in Active Directory on Windows	Yes	msauth_rules.xml	5136, 5137, 5138, 5139, 5141
alienvault-domain_rules.xml	Detect changes in the Domain Admins group on Windows	Yes	msauth_rules.xml	SID: S-1-5-21 domain 512, 518, and 519
alienvault-linux-USB_rules.xml	Detect new USB devices on Linux	No	None	N/A
alienvault-linux-pam_rules.xml	Detect SSHD authentication on Linux	No	None	N/A
alienvault-mssql_rules.xml	Rules for Microsoft SQL Server	No	msauth_rules.xml	14151, 18265, 33205
alienvault-network-login-failure_rules.xml	Detect failed logon attempts on Windows	No	msauth_rules.xml	4625 ⁷
alienvault-sam-express_rules.xml	Rules for SAM (SafeNet Authentication Manager) Express	No	msauth_rules.xml	N/A
alienvault-web-access_rules.xml	Rules to supplement the default web access rules	No	web_rules.xml	N/A
alienvault-windows-ADFS-servers_rules.xml	Rules for Active Directory Federation Services on Windows	No	msauth_rules.xml	1102

AlienVault HIDS Rules (Continued)

Rule File Name	Rules Purpose	Enabled by Default	Rule File Dependency	Windows Event ID Matched
alienvault-windows-DHCP_rules.xml	Detect DHCP lease actions on Windows	No	ms_dhcp_rules.xml	DHCP server event 10, 11, 12, 13, 16, 17, 18, 20, 21, 23, 30, 32
alienvault-windows-FIM_rules.xml	Detect file changes on Windows	Yes	msauth_rules.xml	4659
alienvault-windows-USB_rules.xml	Detect new USB devices on Windows	Yes	ossec_rules.xml	N/A
alienvault-windows-access_rules.xml	Detect Object Access issues on Windows	No	msauth_rules.xml	4656, 4662, 4673, 4674
alienvault-windows-account-security_rules.xml	Detect account activities on Windows	No	msauth_rules.xml	4720, 4722, 4725, 4726, 4738, 4781
alienvault-windows-applocker_rules.xml	Detect AppLocker activities on Windows	No	msauth_rules.xml	8002, 8003, 8004, 8005, 8006, 8007
alienvault-windows-capacity_rules.xml	Detect capacity issues on Windows	No	msauth_rules.xml	2013
alienvault-windows-defender_rules.xml	Rules for Windows Defender	No	msauth_rules.xml, ms-se_rules.xml	1000, 1001, 1116, 1117, 5007
alienvault-windows-filtering_rules.xml	Rules for Windows Filtering Platform (WFP)	No	msauth_rules.xml	5152
alienvault-windows-group-changes_rules.xml	Detect Security group changes in Active Directory on Windows	No	msauth_rules.xml	4735, 4737, 4755
alienvault-windows-logon-logoff_rules.xml	Detect machine log on/off attempts on Windows	Yes	msauth_rules.xml	N/A

AlienVault HIDS Rules (Continued)

Rule File Name	Rules Purpose	Enabled by Default	Rule File Dependency	Windows Event ID Matched
alienvault-windows-password-change-rules.xml	Detect password change attempts on Windows	No	msauth_rules.xml	4723, 4724
alienvault-windows-powershell_rules.xml	Rules for Windows PowerShell commands	No	msauth_rules.xml	800
alienvault-windows-process_rules.xml	Detect new processes on Windows	No	msauth_rules.xml	4688, 4689
alienvault-windows-service-control-manager_rules.xml	Rules for Service Control Manager (Windows)	No	msauth_rules.xml	7036, 7045
alienvault-windows-shutdown_rules.xml	Detect power off attempts on Windows	No	msauth_rules.xml	1074
alienvault-windows-workstation-logon-logoff_rules.xml	Detect user logon/off attempts on Windows	Yes	msauth_rules.xml	528, 540, 672, 673, 4624, 4672, 4768, 4769, 4771
local_rules.xml	A file to hold user-defined HIDS rules. it contains a sample rule initially.	Yes	None by default	N/A

¹Total Cores are available physical cores without hyperthreading enabled.

²To guarantee stable operation, you should increase the RAM if the swap space on the hard disk exceeds 1 GB for extended amount of time. Otherwise data collection and normalization, OTX integration, or vulnerability scanning might fail.

³To deploy USM Appliance version 5.7.3 or later, you must be running ESXi 5.5 or later. Previous version of USM Appliance can be deployed on ESXi 4.0 or later.

⁴Due to the way that OTX™ is managed, otx.alienvault.com does not have a fixed IP address and AT&T Cybersecurity cannot provide the IP range.

⁵The USM Appliance API tries to access www.google.com every five minutes to ensure that the system has an Internet connection.

⁶USM Appliance assumes the component to be offline if no response is received from ping.

⁷ This rule is more granular than the default one in msauth_rules.xml, because it matches the different failure reasons reported by event 4625.

AlienVault delivers new HIDS rules or fixes to existing rules through the bi-weekly [The Threat Intelligence Updates](#). For a complete list of rules enabled by default, go to **Environment > Detection > HIDS > Config > Rules**. USM Appliance displays the enabled rules on the left and disabled rules on the right.

DETECTION

HIDS WIRELESS IDS

OVERVIEW | AGENTS | AGENTLESS | EDIT RULES | CONFIG | HIDS CONTROL

RULES SYSCHECKS CONFIGURATION

(*) Drag & Drop the file you want to add/remove or use [+] and [-] links

ENABLED RULES		DISABLED RULES
alienvault-directory-service_rules.xml	—	alienvault-apache_rules.xml
alienvault-windows-FIM_rules.xml	—	alienvault-domain_rules.xml
alienvault-windows-USB_rules.xml	—	alienvault-mssql_rules.xml
alienvault-windows-logon-logoff_rules.xml	—	alienvault-sam-express_rules.xml
alienvault-windows-workstation-logon-logoff_rules.xml	—	alienvault-windows-access_rules.xml
apache_rules.xml	—	alienvault-windows-capacity_rules.xml
arpwatch_rules.xml	—	alienvault-windows-password-change_rules.xml
attack_rules.xml	—	alienvault-windows-process_rules.xml
cisco-ios_rules.xml	—	alienvault-windows-shutdown_rules.xml
courier_rules.xml	—	asterisk_rules.xml
firewall_rules.xml	—	cimserver_rules.xml
ftpd_rules.xml	—	clam_av_rules.xml
hordeimp_rules.xml	—	dovecot_rules.xml

SAVE

(*) You must restart HIDS for the changes to take effect

You can enable more rules based on your business needs. See [Enabling / Disabling AlienVault HIDS Rules](#).

Additionally, you can edit existing rules or create your own so that they work better in your environment. See [Editing / Creating Custom Rules for AlienVault HIDS](#).

Enabling / Disabling AlienVault HIDS Rules

Before deciding whether to enable or disable an AlienVault HIDS rule, you will want to understand what the rule does first. USM Appliance allows you to view the entire rule file from the web UI.



Note: AlienVault HIDS rules are read-only. You cannot change them.

To view a HIDS rule file

1. Go to **Environment > Detection > HIDS > Edit Rules.**

The screenshot shows the 'Edit Rules' interface in the AlienVault HIDS console. The left sidebar contains a tree view of rule files, with 'alienvault-windows-USB_rules.xml' selected. The main area displays the details for this rule, including its attributes (id: 100051, level: 7) and text nodes (if_sid: 530, match: ossec: output: 'wmic logicaldisk where 'drivetype=2 AND NOT deviceid like 'a\' get deviceid, volumename, description, FileSystem, Size, VolumeSerialNumber', check_diff, description: New USB Device Found.).

2. Select the rule file from the drop-down list.
3. Click the plus (+) sign to extend the nodes, or click a node to display the details in the right column.
4. Alternatively, click the **Rule Editor** tab to see the rule file in XML format.

The screenshot shows the 'Rule Editor' tab in the AlienVault HIDS console. The left sidebar contains the same tree view of rule files. The main area displays the XML code for the selected rule, showing the group name, rule id, level, if_sid, match, check_diff, and description.

Some rules depend on other rules to find their matching events first. Therefore, before you enable a rule, make sure that the dependent rule (as shown in the Rule File Dependency column in the [AlienVault HIDS Rules](#) table) has been enabled. For example, the alienvault-windows-defender_rules.xml file depends on both msauth_rules.xml and ms-se_rules.xml files. While msauth_rules.xml is enabled by default, ms-se_rules.xml is not. Therefore, you must enable ms-se_rules.xml first, and then alienvault-windows-defender_rules.xml.

To enable or disable an AlienVault HIDS rule

1. Go to **Environment > Detection > HIDS > Config > Rules**.
2. To enable a rule, type the name of the rule in the search box.

The number of available rules reduces as you type and USM Appliance finds the match.
3. To locate the rule, either drag the file to the left column or click the plus (+) sign next to the rule.
4. To disable a rule, locate the file in the left column. Either drag the file to the right column or click the minus (-) sign next to the rule.
5. Click **Save**.
6. You must restart the HIDS Service for the changes to take effect:
 - On the same page, click the **HIDS Control** tab, and then click **Restart** on the resulting page.

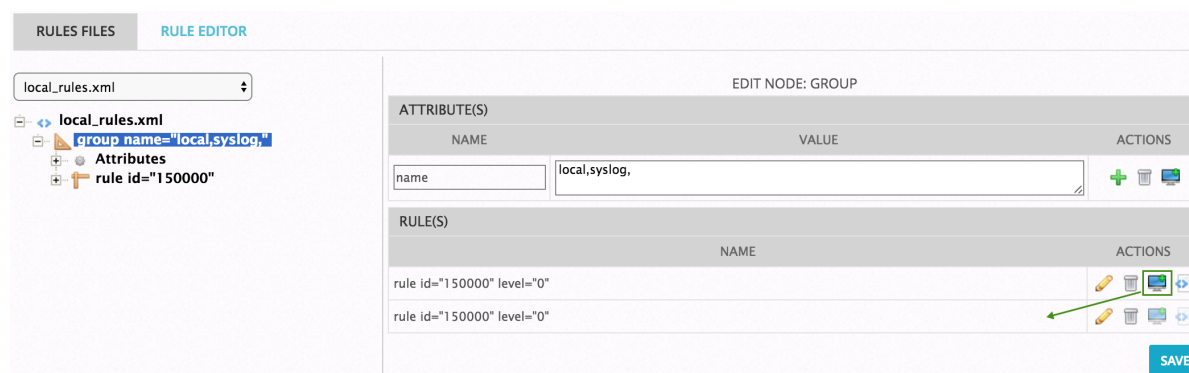
Editing / Creating Custom Rules for AlienVault HIDS

You are not allowed to change any of the AlienVault HIDS rules, but you can create your own rules to detect HIDS issues in your environment. AlienVault recommends that you put your rules in the `local_rules.xml` file, which is enabled by default and loaded at last so that it is not overwritten by the other rule files. You can add or remove rules from `local_rules.xml` in the web UI.

To create or modify a custom HIDS rule

1. Go to **Environment > Detection > HIDS > Edit Rules**.
2. Select `local_rules.xml` from the drop-down list.
3. Click **group name="local,syslog,"** to display the details in the right column.


A sample rule with id 150000 displays.




4. Click the clone rule icon () to clone the sample rule.

Another rule with rule id 150000 displays.


5. Click **Save**.



 **Note:** Save your new rule in order to make changes to it.

6. Click the edit rule icon () next to the newly created rule.

The details of the rule display.







7. Change the **id** so that it is unique.

















 **Important:** A valid custom rule ID for AlienVault HIDS is between **190,000** and **199,999**. AlienVault reserves other ranges for its internal usage.

8. Change the other attributes as needed. Use the add icon () to add an attribute or a node. Use the delete icon () to remove an attribute or a node.


In the example below, we have changed the rule id to 150001 and srcip to 2.2.2.2. We have updated the description as well.

EDIT NODE: RULE

ATTRIBUTE(S)		
NAME	VALUE	ACTIONS
id	150001	  
level	0	  

TEXT NODE(S)		
NAME	VALUE	ACTIONS
if_sid	5711	   
srcip	2.2.2.2	   
description	Example of rule that will ignore sshd	   
description	failed logins from IP 2.2.2.2	   

SAVE

9. If you need to add an attribute for any of the nodes, click the show icon () to display the attributes for that node.
10. Alternatively, if you prefer to use the XML format, click the **Rule Editor** tab and enter your rule directly.

```

1  <group name="local,syslog,">
2    <rule id="150000" level="0">
3      <if_sid>5711</if_sid>
4      <srcip>1.1.1.1</srcip>
5      <description>Example of rule that will ignore sshd</description>
6      <description>failed logins from IP 1.1.1.1.</description>
7    </rule>
8    <rule id="150001" level="0">
9      <if_sid>5711</if_sid>
10     <srcip>2.2.2.2</srcip>
11     <description>Example of rule that will ignore sshd</description>
12     <description>failed logins from IP 2.2.2.2.</description>
13   </rule>
14 </group>
15

```

11. Click **Save** after you have made all the changes.
12. You must restart the HIDS Service for the changes to take effect:
 - On the same page, click the **HIDS Control** tab, and then click **Restart** on the resulting page.

The procedure above shows how to add a new rule to the existing group. If you want to add a new group instead, use the **Rule Editor** and enter the XML codes directly. For example:



The screenshot shows the Rule Editor interface. On the left, a tree view displays the file structure: local_rules.xml, local_rules.xml, group name="local,syslog," and group name="test,". The main area shows the XML code for local_rules.xml, with line numbers 1 through 22. The XML content is as follows:

```

1 <group name="local,syslog,">
2   <rule id="150000" level="0">
3     <if_sid>5711</if_sid>
4     <srcip>1.1.1.1</srcip>
5     <description>Example of rule that will ignore sshd</description>
6     <description>failed logins from IP 1.1.1.1.</description>
7   </rule>
8   <rule id="150001" level="0">
9     <if_sid>5711</if_sid>
10    <srcip>2.2.2.2</srcip>
11    <description>Example of rule that will ignore sshd</description>
12    <description>failed logins from IP 2.2.2.2.</description>
13  </rule>
14 </group>
15 <group name="test,">
16   <rule id="150002" level="0">
17     <if_sid>5711</if_sid>
18     <srcip>3.3.3.3</srcip>
19     <description>Example of rule that will ignore sshd</description>
20     <description>failed logins from IP 3.3.3.3.</description>
21   </rule>
22 </group>

```



Important: Do not add a group without a rule in it. AlienVault HIDS will not restart with an empty group in local_rules.xml.

Tutorial: Reading a Log File with a HIDS Agent on Windows

In this process we will configure an HIDS Agent, installed on a Windows system, to read logs from a file. This can be useful when we try to grab data from an application that logs directly into a file. For this purpose we have created a sample file

C:\Users\WIN7PRO\Desktop\Test.txt with the following log line:

```
"myapplication: This is a test."
```

Task 1. Configure HIDS Agent to read a file on Windows

1. Edit C:\Program Files (x86)\ossec-agent\ossec.conf.
2. Add the following settings inside the <localfile> element of the ossec.conf file:

```

<localfile>
<location>C:\Users\WIN7PRO\Desktop\Test.txt</location>
<log_format>syslog</log_format>
</localfile>

```

3. Restart the ossec-agent service.

Task 2. Enable "logall" on USM Appliance



Note: This task is only required for the initial configuration.

1. In the USM Appliance web UI, go to **Environment > Detection > HIDS > Config > Configuration**.
2. Add `<logall>yes</logall>` to the `<global>` section of the file:

```
<ossec_config>
  <global>
    <email_notification>no</email_notification>
    <custom_alert_output>AV - Alert - "$TIMESTAMP" --> RID:
"$DSTUSER"; SRCIP: "$SRCIP"; HOSTNAME: "$HOSTNAME"; LOCATION
    <logall>yes</logall>
  </global>
```

Adding this setting allows logging of all events to
`/var/ossec/logs/archives/archives.log`.

3. Click **Save** at the bottom of the screen.
4. Restart the HIDS Service:
 - a. Go to **Environment > Detection > HIDS > HIDS Control**.
 - b. Click **Restart**.

Task 3. Confirm that USM Appliance receives the log line

1. Write a new log line in the `Test.txt` file and save, e.g. "myapplication: This is a test 2."
2. On USM Appliance, check for the newly added line in `/var/ossec/-logs/archives/archives.log`.

You can check for log line by running the following command:

```
cat /var/ossec/logs/archives/archives.log | grep -i "myapplication"
```

You should see an output similar to the following:

```
cat /var/ossec/logs/archives/archives.log | grep -i "myapplication"
2015 Jun 16 06:20:30 (TEST) 192.168.1.20->\Users\WIN7PRO\Desktop\Test.txt
myapplication: This is a test 2
```

Task 4. Create a new decoder on USM Appliance to parse the incoming log lines

1. On USM Appliance edit `/var/ossec/alienvault/decoders/local_decoder.xml` (same as `decoder.xml` but this one is not overwritten when updating the system).

If this file does not exist you can create it with the following command:

```
touch /var/ossec/alienvault/decoders/local_decoder.xml
```

2. In `local_decoder.xml` add a new decoder to parse first part of the log message and save your changes:

```
<decoder name="myapplication">
<prematch>^myapplication: </prematch>
</decoder>
```

3. In the USM Appliance web UI, go to **Environment > Detection > HIDS > Config > Configuration**.
4. Add `<decoder>alienvault/decoders/local_decoder.xml</decoder>` right after `<decoder>`:

```
<ossec_config> <!-- rules global entry -->
<rules>
<decoder>alienvault/decoders/decoder.xml</decoder>
<decoder>alienvault/decoders/local_decoder.xml</decoder>
</rules>
</ossec_config> <!-- rules global entry -->
```

Adding this setting enables the usage of a custom decoder.

5. Click **Save** at the bottom of the screen.
6. Restart the HIDS service as detailed in Task 2 Step 4.
7. Run `/var/ossec/bin/ossec-logtest` and paste the log line "myapplication: This is a test."
8. Check if it recognizes the decoder.

If it works you will see the newly created decoder listed.

Task 5. Create a new rule on USM Appliance to parse lines processed by the decoder



Important: Use a number between 190,000 and 199,999 as the `rule id`.

1. On USM Appliance edit `/var/ossec/alienvault/rules/local_rules.xml`.
2. Add the following lines to the file:

```
<group name="myapplication">
<rule id="196000" level="0">
<decoded_as>myapplication</decoded_as>
<description>myapplication is enabled</description>
</rule>

<rule id="196001" level="1">
<if_sid>196000</if_sid>
<match>Test</match>
<description>Test string found</description>
</rule>
</group>
```

3. Restart the HIDS service as detailed in Task 2 Step 4.
4. Run `/var/ossec/bin/ossec-logtest` and paste a log line (in this case "myapplication: This is another Test").
5. Check if it recognizes the rule:

You will see Phase 3 of the Log Test has completed and matched our new rule:

```
USM:~# /var/ossec/bin/ossec-logtest
2015/06/16 07:22:07 ossec-testrule: INFO: Reading local decoder file.
2015/06/16 07:22:07 ossec-testrule: INFO: Started (pid: 11121).
ossec-testrule: Type one log per line.

myapplication: This is another Test

**Phase 1: Completed pre-decoding.
  full event: 'myapplication: This is another Test'
  hostname: 'USM'
  program_name: '(null)'
  log: 'myapplication: This is another Test'

**Phase 2: Completed decoding.
  decoder: 'myapplication'

**Phase 3: Completed filtering (rules).
  Rule id: '106001'
  Level: '1'
  Description: 'Test string found'
**Alert to be generated.
```

Task 6. Create and configure local version of the ossec-single-line plugin

1. Create a `.local` version of the `ossec-single-line` plugin (if it does not already exist) and ensure it has the correct owner, group and permissions:

```
touch /etc/ossim/agent/plugins/ossec-single-line.cfg.local
chown root:alienvault /etc/ossim/agent/plugins/ossec-single-line.cfg.local
chmod 644 /etc/ossim/agent/plugins/ossec-single-line.cfg.local
```

2. Insert or add the following translation to the `ossec-single-line.cfg.local` file:

```
[translation]
196001=7999
```

3. Insert a new `plugin_sid` with value "196001" for the `ossec-single-line` plugin. This can be done using the following command:

```
echo 'INSERT IGNORE INTO plugin_sid(plugin_id, sid, category_id, class_id,
reliability, priority, name) VALUES(7999, 196001, NULL, NULL, 1, 2,
"ossec: my_application_test_rulematch");' | ossim-db
```

4. Run the command below to ensure the new configuration takes effect :

```
alienvault-reconfig
```

Task 7. Test your configuration

1. Generate new logs and check `/var/ossec/logs/alerts/alert.log` while the logs are being written to the file:

```
tailf /var/ossec/logs/alerts/alerts.log | grep myapplication
```

You should see an output similar to the following, which confirms correct operation:

```
tailf /var/ossec/logs/alerts/alerts.log | grep myapplication
AV - Alert - "1434530803" --> RID: "196001"; RL: "1"; RG:
"ourapplication"; RC: "Test string found"; USER: "None"; SRCIP: "None";
HOSTNAME: "(TEST) 192.168.1.20->\Users\WIN7PRO\Desktop\Test.txt";
LOCATION: "(TEST) 192.168.1.20->\Users\WIN7PRO\Desktop\Test.txt"; EVENT: "
[INIT]myapplication: This is a test log[END]";
AV - Alert - "1434530829" --> RID: "196001"; RL: "1"; RG:
"ourapplication"; RC: "Test string found"; USER: "None"; SRCIP: "None";
HOSTNAME: "(TEST) 192.168.1.20->\Users\WIN7PRO\Desktop\Test.txt";
LOCATION: "(TEST) 192.168.1.20->\Users\WIN7PRO\Desktop\Test.txt"; EVENT: "
[INIT]myapplication: This is another test log[END]";
```

2. (Alternatively) Generate new logs and look in the USM Appliance web UI for results:

- a. Go to **Analysis > Security Events (SIEM)**.
- b. Under **Datasource**, select "AlienVault HIDS".
- c. Click **Grouped** to view the events in groups.

You should see the newly created events with the event name: **AlienVault HIDS: my_application_test_rulematch**.

Task 8. Disable "logall"

Repeat all actions taken in [Task 2. Enable "logall" on USM Appliance](#), but this time delete the line "<logall>yes</logall>" from `ossec.conf`. This is to prevent the `archives.log` file from growing too large.

Task 9. (Optional) Enable File Integrity Monitoring (FIM)

For details on how to configure FIM, see [File Integrity Monitoring](#).

Uninstalling AlienVault HIDS Agents


USM Appliance and AlienVault OSSIM provide host intrusion detection services (HIDS) functionality using AlienVault HIDS Services. The service is extended through HIDS agents installed on Linux or Windows hosts. USM Appliance simplifies the installation of these HIDS agents by providing an automatic deployment script for Windows Hosts. However, due to the nature of how remote install is executed on Windows systems, this functionality can't be extended to uninstalling the agents.

To uninstall an HIDS agent

1. Login to the host and uninstall the program:
 - On Windows:
 - a. Go to the Control Panel.
 - b. Select **Programs > Uninstall a program**.
 - c. Select the program named *OSSEC HIDS 2.9.1* and click **Uninstall**.
 - On Linux:

- a. Run the following command

```
/var/ossec/bin/ossec-control stop && rm -rf /var/ossec && rm
/etc/init.d/*ossec* && rm /etc/ossec-init.conf
```

2. In USM Appliance, go to **Environment > Detection**.
3. Click the **Agents** tab to see a list of agents.
4. Select the agent that you've uninstalled and click the trash can icon () to remove it from the list.
5. After you've removed all the agents, click the **HIDS Control** tab, and then click **Restart** to restart the HIDS service.

If you wish to remove the HIDS agent from multiple hosts, you'll need to use a third-party tool or script to facilitate bulk removal. If your organization is using any group policy for administration, you may want to discuss using a Windows Management Instrumentation Command-line (WMIC) script governed by a group policy object (GPO). Please contact your Active Directory administrator or consultant for more information on how to use this Windows feature.

Agent removal for Linux hosts may also be managed by a number of package installation utilities. Please contact your Linux Administrator to determine if your organization is utilizing a package management solution that can facilitate bulk removal.

AlienVault NIDS

- [AlienVault NIDS](#)
- [Configuring AlienVault NIDS](#)
- [Viewing AlienVault NIDS Events](#)
- [Customize AlienVault NIDS Rules](#)
- [Updating AlienVault NIDS Rules and Signatures](#)

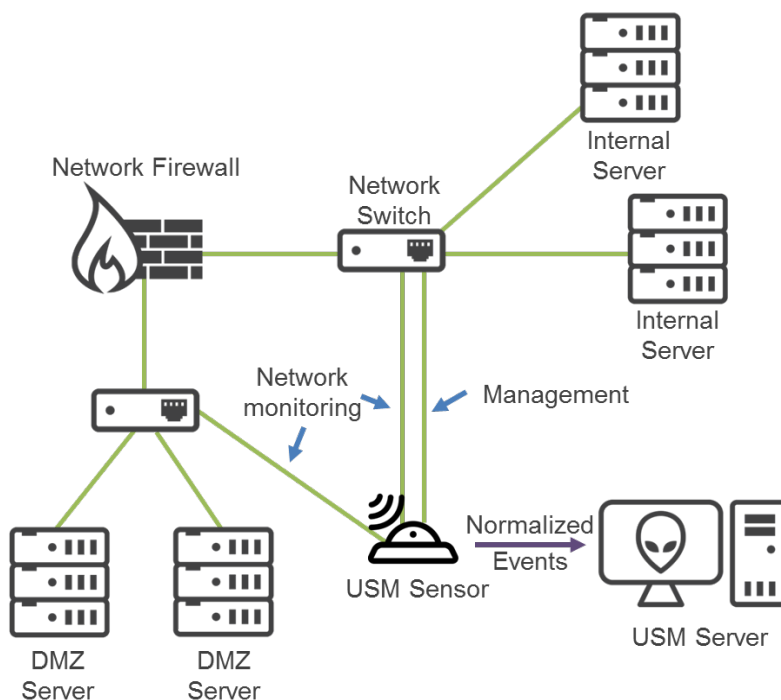
AlienVault NIDS

AlienVault NIDS plays an important role in the USM Appliance. By detecting malicious network events, it provides vital information for correlation directives and cross-correlation rules. Combining this information with the events collected from other devices, USM Appliance presents a complete picture of the malicious activity.

The AlienVault NIDS functionality, including monitoring network traffic and detecting malicious events, takes place on the USM Appliance Sensor. You should configure at least two network interfaces on a USM Appliance Sensor or USM Appliance All-in-One:

- Management interface — Configure the interface with an IP address, which you can reach from the network. Use this interface for administrative purposes and communication with other USM Appliance components. See [Set Up the Management Interface](#).
- Network monitoring interface — Do not configure an IP address on the interface. Instead, connect the interface to a spanned or mirrored port on a network switch, so that USM Appliance can examine the throughput. You can use more than one network monitoring interface to observe several networks from a single USM Appliance Sensor. See [Configuring AlienVault NIDS](#).

The USM Appliance Server consumes the NIDS signatures through plugins, which generates the AlienVault NIDS events. The correlation engine processes and correlates the normalized events, then stores them in the SIEM database.



AlienVault NIDS diagram

Configuring AlienVault NIDS

USM Appliance comes with AlienVault NIDS already enabled, but you need to perform the steps below in order to monitor network traffic.

1. Enable one or more interfaces for monitoring
2. Add monitored networks
3. Using SPAN or mirror ports, configure your network devices to send traffic to the monitoring interface.



Important: AT&T Cybersecurity recommends that you send packets *untagged* through the SPAN/mirror port. This is because VLAN trunking is currently not supported. Therefore, Bridge Protocol Data Units (BPDUs) or packets sent through the other Layer 2 protocols are dropped. The Layer 2 protocols include, but are not limited to, Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), Link Aggregation Control Protocol (LACP), Port Aggregation Protocol (PAgP), Spanning Tree Protocol (STP), and VLAN Trunk Protocol (VTP).

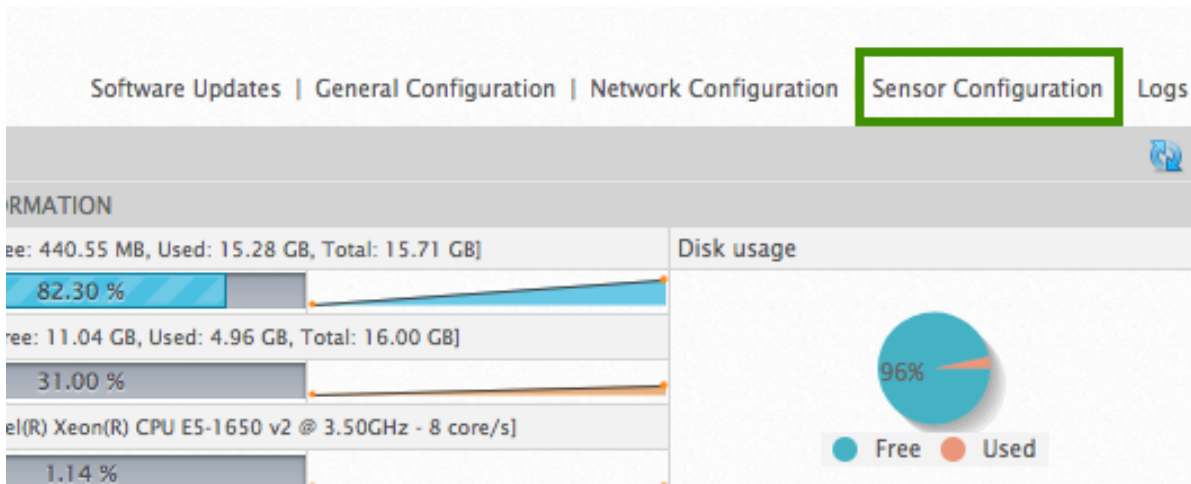
Enable a Network Interface for Monitoring

If you have a USM Appliance All-in-One and you have not completed the initial configuration, you can enable the interface for NIDS monitoring by using the Getting Started Wizard. See [Configuring Network Interfaces](#).

Otherwise, you can configure the network interface by using the web UI (recommended) or the AlienVault Setup menu.

To enable an interface using the web UI

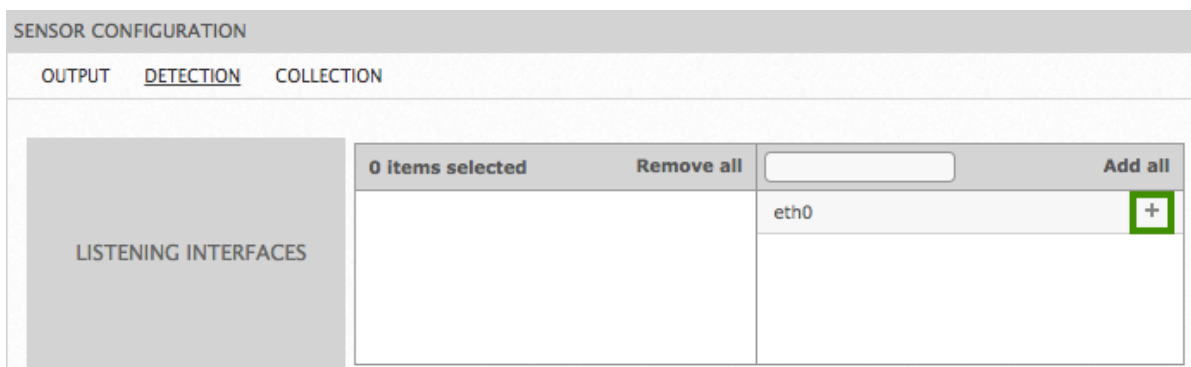
1. Go to **Configuration > Deployment > Components > AlienVault Center**.
2. Double-click the instance you want to configure.
3. Click **Sensor Configuration**.



- Click **Detection**.



- In the **Listening Interfaces** area, click the plus (+) sign next to the interface you want to add.

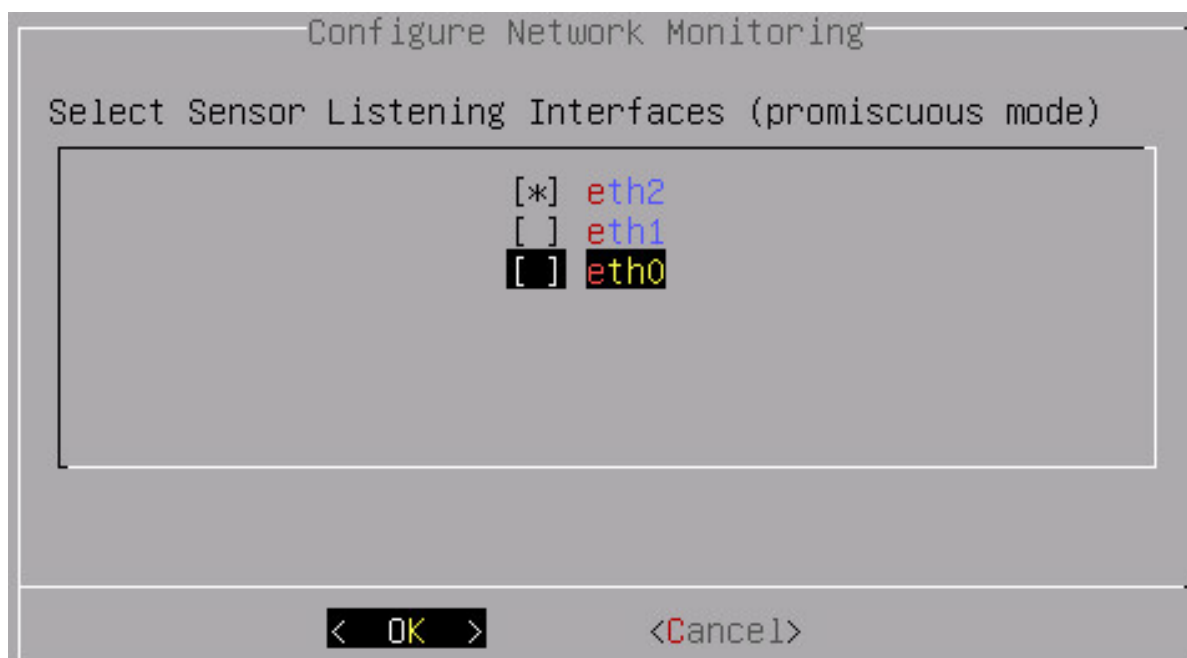


- Click **Apply Changes**.

To enable an interface in the AlienVault Setup menu

- Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
- Select **Configure Sensor**.
- Select **Configure Network Monitoring**.

4. Use the keyboard arrow keys to move to the interface, select the interface by pressing the spacebar, and then press Enter (<OK>).



5. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
6. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Add Monitored Networks

By default, USM Appliance monitors all RFC 1918 private networks (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). Therefore, you do not need to take any further actions if your network uses private IP addresses. However, if you want to monitor a network with public IP addresses, you have to add the network to the list of monitored networks. You can add a network for NIDS monitoring by using the web UI (recommended) or the AlienVault Setup menu.

To add a network using the web UI

1. Go to **Configuration > Deployment > Components > AlienVault Center**.
2. Double-click the appliance you want to configure.
3. Click **Sensor Configuration**.
4. Click **Detection**.

5. In **Monitored Networks**, type the network address and click **Add**.

MONITORED NETWORKS	
1.1.1.1	ADD
192.168.0.0/16	
172.16.0.0/12	
10.0.0.0/8	

6. Click **Apply Changes**.

To add a network in 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 **Configure Sensor**.
3. Select **Network CIDRs**.
4. Type the network addresses you want to monitor, separating with comma, and then press Enter (<OK>).

Network CIDRs

Enter Monitored Networks (CIDRs separated by ,)
i.e. 127.0.0.0/24,192.168.0.0/16

192.168.0.0/16,172.16.0.0/12,10.0.0.0/8,192.0.2.0/24,198.51.100.0/24

< OK > <Cancel>

5. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
6. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

Viewing AlienVault NIDS Events

You can view AlienVault NIDS events the same way as you do any other security events. For reference, see "Security Events (SIEM) Views" in the Event Management section of the *USM Appliance User Guide*.

To view AlienVault NIDS events

1. Go to **Analysis > Security Events (SIEM) > SIEM**.
2. From the **Data Sources** list, select AlienVault NIDS.

The screenshot shows the AlienVault NIDS SIEM interface. The top navigation bar includes DASHBOARDS, ANALYSIS (selected), ENVIRONMENT, REPORTS, and CONFIGURATION. Below the navigation bar, the 'SECURITY EVENTS (SIEM)' section is active, with tabs for SIEM, REAL-TIME, and EXTERNAL DATABASES. A search bar is present with a 'GO' button. The 'SHOW EVENTS' section on the left includes radio buttons for 'Last Day', 'Last Week', 'Last Month', and 'Date Range'. The main filter area contains several dropdown menus: DATA SOURCES (set to 'AlienVault NIDS'), DATA SOURCE GROUPS, ASSET GROUPS, NETWORK GROUPS, OTX IP REPUTATION, OTX PULSE, and RISK. There are also checkboxes for 'EXCLUDE' and 'ONLY OTX PULSE ACTIVITY'. A 'CLEAR FILTERS' button is on the right. Below the filters, there are tabs for 'EVENTS', 'GROUPED', and 'TIMELINE'. The 'EVENTS' tab is selected, showing a table of events. The table has columns for SIGNATURE, DATE GMT-4:00, SENSOR, OTX, SOURCE, DESTINATION, and RISK. Three events are listed, all with a risk level of 0. The first event is 'AlienVault NIDS: "ET POLICY Suspicious inbound to MSSQL port 1433"'. The second is 'AlienVault NIDS: "ET POLICY Suspicious inbound to PostgreSQL port 5432"'. The third is 'AlienVault NIDS: "ET POLICY Suspicious inbound to Oracle SQL port 1521"'. At the bottom right, there are buttons for 'CHANGE VIEW' and 'ACTIONS'.

SIGNATURE	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
AlienVault NIDS: "ET POLICY Suspicious inbound to MSSQL port 1433"	2015-09-11 07:09:57	VirtualUSMAllInOne	N/A	1.1.1.2:34143	Server2008:1433	0
AlienVault NIDS: "ET POLICY Suspicious inbound to PostgreSQL port 5432"	2015-09-11 07:09:56	VirtualUSMAllInOne	N/A	1.1.1.2:34143	Server2008:5432	0
AlienVault NIDS: "ET POLICY Suspicious inbound to Oracle SQL port 1521"	2015-09-11 07:09:54	VirtualUSMAllInOne	N/A	1.1.1.2:34143	Server2008:1521	0

AlienVault NIDS events suggest that an attack may have occurred, but they don't guarantee that such attack has occurred. Therefore, you must examine the traffic that triggered the signature and validate the malicious intent, before proceeding with your investigation.

At the bottom of the event details page, all AlienVault NIDS events include a payload and the rule that identified the issue. You can examine the payload of the offending packet, study the rule, or download the PCAP file for off-line analysis.

PAYLOAD

```

length = 168
000 : 47 45 54 20 2F 43 46 49 44 45 2F 63 6F 6D 70 6F GET /CFIDE/compo
010 : 6E 65 6E 74 75 74 69 6C 73 2F 63 66 63 65 78 70 nentutils/crcexp
020 : 6C 6F 72 65 72 2E 63 66 63 20 48 54 50 2E 31 lorer.cfo HTTP/1
030 : 2E 31 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 .1..Connection:
040 : 4B 65 65 70 2D 41 6C 69 76 65 0D 0A 55 73 65 72 Keep-Alive..User
050 : 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F -Agent: Mozilla/
060 : 35 2E 30 30 20 28 4E 69 6B 74 6F 2F 32 2E 31 2E 5.00 (Nikto/2.1.
070 : 35 29 20 28 45 76 61 73 69 6E 73 3A 4E 6F 6E 5) (Evasions:Non
080 : 65 29 20 28 54 65 73 74 3A 30 30 35 39 32 29 e) (Test:008592)
090 : 0D 0A 48 6F 73 74 3A 20 31 30 2E 34 37 2E 33 30 ..Host: 10.47.30
0A0 : 2E 31 30 32 0D 0A 0D 0A .102....

```

Rule Detection

```

File: emerging_pro-web_server.rules
Rule: alert http any any -> $HTTP_SERVERS any
msg: "ET WEB_SERVER ColdFusion componentutils access"
flow: established,to_server
content: "GET"
http_method:
nocase:
content: "/CFIDE/componentutils"
http_uri:
nocase:
reference: url,www.adobe.com/support/security/advisories/apsa13-01.html
classtype: web-application-attack
sid: 2016182
rev: 6

```

PCAP FILE [\[DOWNLOAD IN PCAP FORMAT\]](#)

Customize AlienVault NIDS Rules

Occasionally you may want to customize the AlienVault NIDS rules or enable a rule that is disabled by default, so that the detection works better in your network. This section describes how to accomplish both.



Important: The steps below have been written for the USM Appliance All-in-One.

If running the USM Appliance Server and USM Appliance Sensor separately, you must perform step #1 through #7, step #9, and step #10 on each Sensor. You must perform step #8 on the USM Appliance Server, after copying the `local.rules` file from the Sensor to the Server. This is because the database only exists on the Server.

To customize the AlienVault NIDS rule(s)

1. Identify the rule(s) you want to enable.
2. Connect to the AlienVault Console through `SSH` and use your credentials to log in. The AlienVault Setup menu displays.
3. 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.

4. Place the rule you want to enable into `/etc/suricata/rules/local.rules` and save your changes. One way to do this is to copy the rule(s) from the original rule file and paste it into `local.rules`, making sure to remove the `"#"` at the beginning of the line.

The following example performs these tasks in a Linux one-liner

```
# cat /etc/suricata/rules/emerging_pro-policy.rules | grep 2009294 | cut -d'#' -f2 >> /etc/suricata/rules/local.rules
```

In this command, `grep` is used to search for the unique ID of a disabled Credit Card Policy Rule, copy it from `/etc/suricata/rules/emerging_pro-policy.rules`, remove the `"#"` at the beginning of the line (using `cut`), and paste it to `/etc/suricata/rules/local.rules`.

Open `local.rules` to confirm that the rule was copied correctly

```
# cat /etc/suricata/rules/local.rules
alert ip any any > any any (msg:"ET POLICY Credit Card Number Detected in Clear (15 digit dashed 2)"; pcre:"/ (3[4|7]\d{2}|2014|2149|2131|1800)-\d{6}-\d{5} /"; reference:url,www.beachnet.com/~hstiles/cardtype.html; reference:url,doc.emergingthreats.net/2009294; classtype:policy-violation; sid:2009294; rev:1;)
```



Note: To ensure that the rule doesn't conflict with existing rules, you should use a SID between 5,000,000 and 5,999,999.

5. Repeat the command for all the rules you want to enable.
6. Modify the rule(s) if needed and save your changes.
7. Using a command line text editor of your choice, add a reference to `local.rules` at the bottom of `/etc/suricata/rule-files.yaml`

```
%YAML 1.1
---
default-rule-path: /etc/suricata/rules
rule-files:
- emerging_pro-activex.rules
- emerging_pro-attack_response.rules
- emerging_pro-chat.rules
[...]
- suricata-smtp-events.rules
- suricata-stream-events.rules
- local.rules
```

8. Run the following script to import the rules to the database

```
perl /usr/share/ossim/scripts/create_sidmap.pl /etc/suricata/rules
```

9. Restart the AlienVault NIDS service for your changes to take effect

```
#service suricata restart
```

10. Restart the AlienVault Agent service to digest the changes

```
#service ossim-agent restart
```



Warning: If you are using USM Appliance version 5.3.3 or earlier, running threat intelligence or plugin feed updates will overwrite any changes you made to the `local.rules` file. To avoid this issue, upgrade to USM Appliance version 5.3.4 or later.

Updating AlienVault NIDS Rules and Signatures

The AT&T Alien Labs™ Security Research Team provides threat intelligence updates, such as new Intrusion Detection System (IDS) rules and signatures, to customers running USM Appliance version 5.4.3 or later.

To detect the latest threats with AlienVault NIDS, you should keep the IDS signatures in USM Appliance up-to-date. USM Appliance checks for threat intelligence updates every 15 minutes. Once an update becomes available, a message appears in the Message Center. For details, see "About the Message Center" in the *USM Appliance Deployment Guide*.

To see if USM Appliance has a new or updated NIDS signature available

1. Open the Message Center.
2. Search for any messages that contain "AlienVault Labs Threat Intelligence" in the message subject.
3. Click the message and read about the added NIDS signatures.

Open Message Center

Search for a message

Added NIDS signatures

MESSAGE CENTER

Search

Unread (28)
All Messages (31)

Message Type

- ☐ Update (4)
- ☐ Deployment (4)
- ☐ Information (2)
- ☐ AlienVault (18)

Priority

- ☐ Info (27)
- ☐ Warning (1)
- ☐ Error (0)

DATE	SUBJECT	PRIORITY	TYPE	ACTIONS
2015-06-01 20:00:00	New Update: AlienVault 5.0.3 has been released	info	Update	
2015-05-31 20:00:00	AlienVault Labs Threat Intelligence Update - Week of May 24th, 2015	info	AlienVault	
2015-05-25 20:00:00	Become an AlienVault Certified Security Engineer	info	Information	
2015-05-18 20:00:00	AlienVault Labs Threat Intelligence Update - 05-18-2015	info	AlienVault	
2015-05-13 20:00:00	AlienVault Labs Threat Intelligence Update - 05-13-2015	info	AlienVault	
2015-04-15 05:39:51	Customer training webcast	info	AlienVault	

AlienVault Labs Threat Intelligence Update – 05-18-2015

2015-05-18 20:00:00

Correlation rules added

- 41356 System Compromise Malware infection RADMINRMS
- 41354 System Compromise Targeted Malware Hellsing
- 41355 System Compromise Trojan infection FrauDrop
- 41352 System Compromise Trojan infection Chaori
- 41353 System Compromise Trojan infection Bomjogo

Correlation rules modified

- 32003 Environmental Awareness Desktop Software – P2P eDonkey
- 40154 System Compromise Trojan infection Banload
- 41301 System Compromise C&C Communication Known malicious SSL certificate
- 41309 System Compromise Malware infection CoinMiner
- 41335 System Compromise C&C Communication Dridex SSL Certificate
- 32122 Environmental Awareness Anonymous channel Tor Onion Proxy
- 40051 System Compromise Trojan infection Bancos
- 41301 System Compromise C&C Communication Known malicious SSL certificate
- 41309 System Compromise Malware infection CoinMiner
- 32122 Environmental Awareness Anonymous channel Tor Onion Proxy

Network Intrusion Detection Signatures added

- 2021097 ET TROJAN Win32/Ruckguy.A SSL Cert
- 2021096 ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Malware CnC)
- 2021099 ET MALWARE PUP.GigaClicks Checkin
- 2021098 ET TROJAN Win32/Troldesh.A SSL Cert
- 2811007 ET PRO TROJAN CoinMiner Known malicious stratum authline (482fe401)
- 2811006 ET PRO TROJAN CoinMiner Known malicious stratum authline (AkiraKiku.4)
- 2811005 ET PRO TROJAN BACKDOOR.RADMINRMS.WIN32.1 Checkin POST
- 2811004 ET PRO TROJAN BACKDOOR.RADMINRMS.WIN32.1 CnC
- 2811003 ET PRO MALWARE W32/Banload.UOL/tr.dldr Checkin
- 2811002 ET PRO MALWARE Win32/Bomjogo.A Checkin
- 2811001 ET PRO TROJAN Win32.Dizkatun Checkin
- 2811000 ET PRO MALWARE Win32/Bancos.YW Checkin

After you have reviewed the information in a threat intelligence update and decided to install it, you need to run the update manually either through the web interface (recommended) or the AlienVault Setup menu.

To install threat intelligence updates using the web interface

1. Go to **Configuration > Deployment > Components > AlienVault Center**.
2. Click the yellow arrow in the **New Updates** column next to the USM Appliance you want to install the updates on.
3. Examine the available updates.

NIDS updates contain “suricata” in the package name.

4. Click **Update Feed Only**.



Note: This updates signatures and rules for all packages listed in the update summary, not just the IDS signatures.

The upgrade process can take several minutes. After completion, the page displays a message indicating a successful update.

To install threat intelligence updates in the AlienVault Setup Menu

1. Launch the AlienVault console.
2. Select **System Preferences**.
3. Select **Update AlienVault System**.
4. Select **Update Threat Intelligence**.
5. Confirm your selection.




Note: The AlienVault console does not show the list of available updates, but you can check the update progress.

The upgrade process can take several minutes. After completion, the console displays a message indicating a successful update.

VPN Configuration

Establishing a Virtual Private Network (VPN) connection between AlienVaultUSM Appliance components encrypts all network traffic that passes through a secure VPN tunnel. The AlienVault VPN environment consists of a single VPN server that connects to at least one, but usually multiple, VPN clients. In general, you configure a USM Appliance Server (Standard or Enterprise) or an USM Appliance All-in-One to act as the VPN server.

 **Important:**

- A USM Appliance system cannot serve both as a VPN server and a VPN client at the same time.
- You cannot configure a [USM Appliance Enterprise Server](#) to be the VPN client.

This section covers the following subtopics:

Prerequisites	176
Configure a VPN Between USM Appliance Systems	176
Building a VPN Tunnel Without a Client-Server Connection	180
Verifying the VPN Connection	183
Disabling a VPN Configuration	183

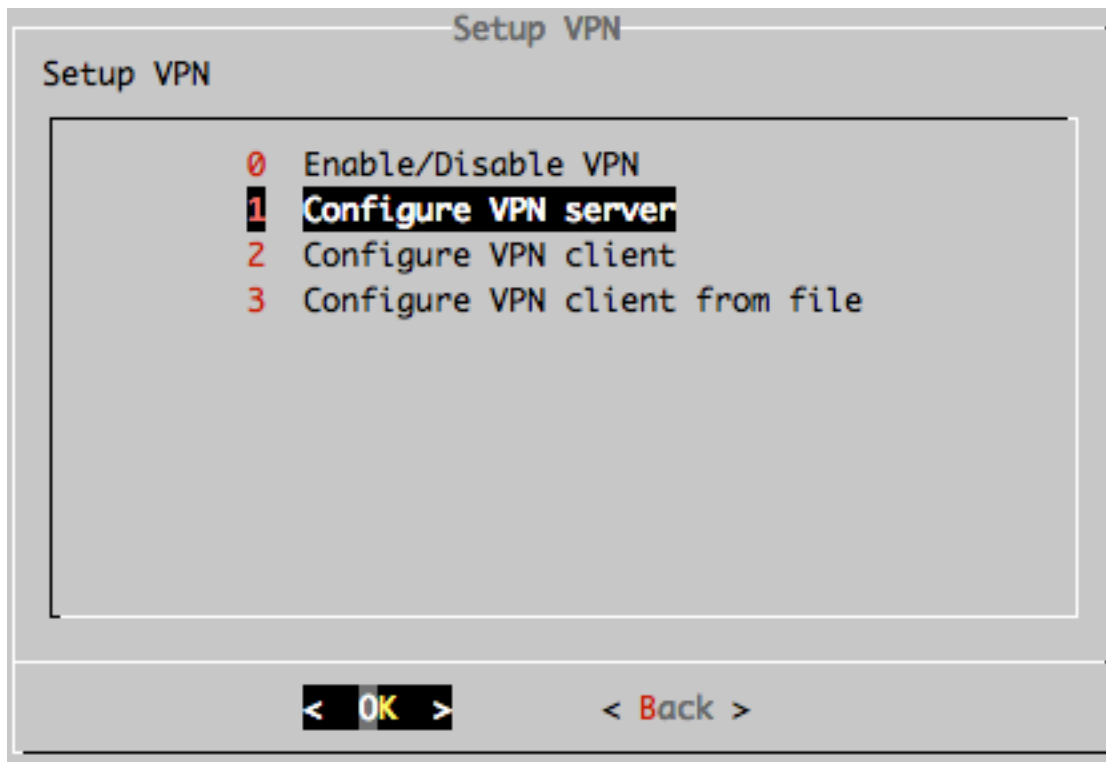
Prerequisites

You must have already set up your USM Appliance Server, USM Appliance Sensor, or USM Appliance Logger, with one exception. If you intend for your Sensor or Logger to act as the VPN client, you only complete setup up to, but *not including*, the tasks in [Configure the USM Appliance Sensor after Deployment](#) or [Configure the USM Appliance Logger after Deployment](#), as applicable.

Before completing that configuration task, you must have first created a VPN tunnel between the VPN server and VPN client. This gives you the VPN IP address required to configure the Sensor or Logger in that role.

Configure a VPN Between USM Appliance Systems

To set up a VPN between two USM Appliance components, for example, between a USM Appliance All-in-One and a USM Appliance Sensor, or between a USM Appliance Server and a USM Appliance Logger, you need to configure through the AlienVault Setup menu, on the **System Preferences > Configure Network > Setup VPN** screen:





Note: You must have completed the [USM Appliance registration](#) to see the VPN-related configuration options in the AlienVault Setup menu.

If setting up VPN in USM Appliance version 5.0 or earlier, you first enable VPN, then configure the VPN server.

If setting up VPN in USM Appliance version 5.1 or later, these tasks are reversed, with the VPN server configuration first, then VPN enablement.

Configure a VPN Server

When you configure a VPN server, you create the VPN interface by specifying the following parameters:

- Virtual network IP — 10.67.68
- VPN network mask IP — 255.255.255.0
- VPN port — 33800

To configure the VPN server

1. Log in either locally or remotely to the AlienVault appliance that you want to act as the VPN server.
2. From the Setup Main menu, go to **System Preferences > Configure Network > Setup VPN > Configure VPN server**, then press **Enter** (<OK>).
3. On the **Configure VPN server** screen, press **Enter** (<Yes>) again.
4. Enter a virtual network IP to use and press **Enter** (<OK>).



Note: By default, the network IP is always 10.67.68.

5. Enter a VPN mask and press **Enter** (<OK>).



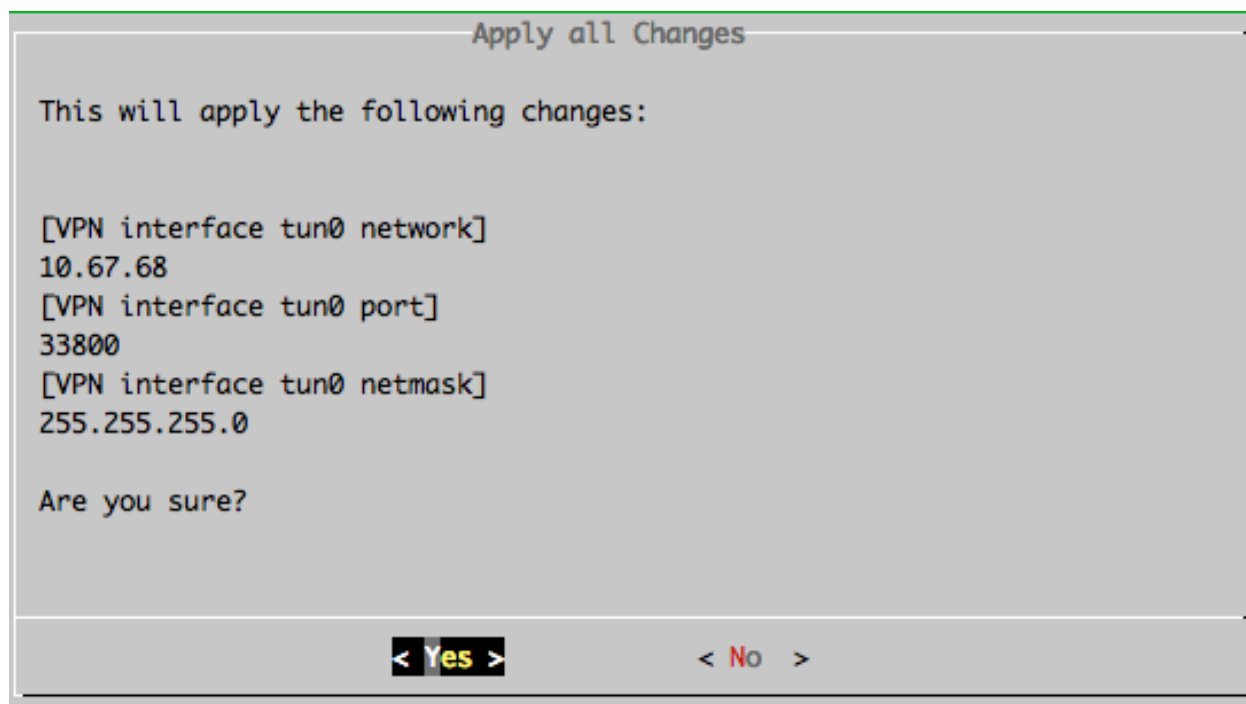
Note: By default the mask is always 255.255.255.0

6. Enter a VPN port and press **Enter** (<OK>).



Note: By default, it is always 33800.

7. Use the **<Back>** option and press **Enter** until the AlienVault Setup menu reappears.
8. Go to **Apply all Changes** and press **Enter** (<OK>):



9. Press **Enter** (<Yes>) to confirm.

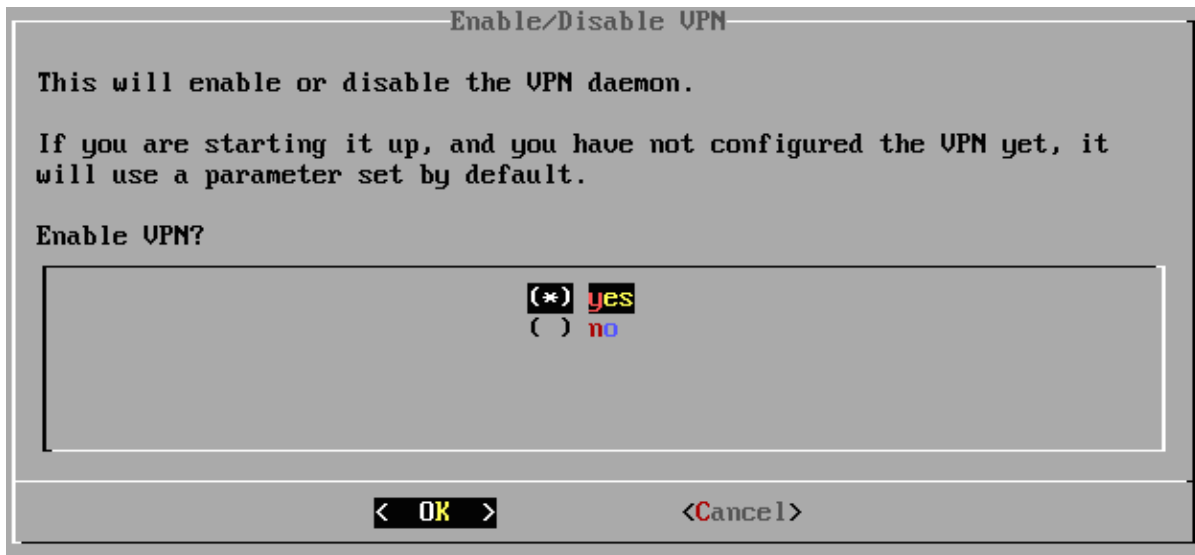
The system applies the changes and restart the services, then console displays: Changes Applied.

10. Press **Enter** (<OK>).

Enabling VPN

To enable the VPN

1. From the AlienVault Setup Main menu, go to **System Preferences > Configure Network > Setup VPN > Enable/Disable VPN**, then press **Enter** (<OK>).
2. Use the arrow keys to move the asterisk(*) to "yes", press the spacebar to select, and then press Enter (<OK>).



3. Press **Enter** (<OK>) again.
4. Use the **<Back>** option and press **Enter** until the AlienVault Setup menu reappears.
5. Go to **Apply all Changes** and press **Enter** (<OK>).

Create the VPN Client

You must complete the following VPN client creation tasks in the order presented:

Build a VPN Tunnel

This task builds a tunnel between the configured VPN server and the node intended to act as the VPN client.

To build a tunnel between the VPN server and a client

1. Log in either locally or remotely to the VPN server appliance.
2. From the Setup Main menu, go to **System Preferences > Configure Network > Setup VPN > Configure VPN client**.
3. Press **Enter** (<OK>).
4. Enter the Administration IP Address of the VPN client, and press **Enter** (<OK>).
5. Enter the root password of the remote system, and press **Enter** (<OK>).
6. Press **Enter** (<Yes>) to confirm.

The system confirms that the VPN client node was successfully contacted:

```

Building the VPN node configuration...
Restarting OpenVPN server...
Retrieving the local vpn server ip...
Trying to deploy the VPN configuration on the remote AlienVault appliance...
Extracting the remote AlienVault appliance VPN configuration...
Restarting remote OpenVPN service...
Restarting ossim-server
Set VPN IP on the system table
New Node VPN IP 10.67.68.10
Restarting ossim-framework
VPN node successfully connected.
Press [Enter] to continue_

```



Note: Make note of the VPN IP address, because you will need it for the client configuration task.

7. To continue, press **Enter**.

If the tunnel creation process does not finish successfully, the following message appears instead:

```

Trying to deploy the VPN configuration on the remote AlienVault appliance...
An error occurred while establishing the vpn tunnel:
Currently there is no connectivity with the remote AlienVault appliance.
* A new VPN configuration file has been created for the remote AlienVault
* Copy this configuration file to the remote AlienVault appliance at /etc

```

In this case, see [Building a VPN Tunnel Without a Client-Server Connection](#).

Complete the VPN Client Configuration

If the VPN client you are configuring is a USM Appliance Sensor or USM Appliance Logger, you need to finish the configuration by performing some additional steps. Click the corresponding link below for details.



Important: Make sure to use the **VPN IP address** you noted from the output in [step 6](#) in creating the VPN client.

- [Configure the USM Appliance Sensor after Deployment](#)
- [Configure the USM Appliance Logger after Deployment](#)

Building a VPN Tunnel Without a Client-Server Connection

If there is no connection between the VPN server and the client, which is often the case in an MSSP (Managed Security Service Provider) environment, an error occurs when you try to configure the client:

```
Building the VPN node configuration...
Restarting OpenVPN server...
Retrieving the local vpn server ip...
Trying to deploy the VPN configuration on the remote AlienVault appliance...
An error occurred while establishing the vpn tunnel:
Currently there is no connectivity with the remote AlienVault appliance. The
steps to deploy the VPN client manually are the following:
* A new VPN configuration file has been created for the remote AlienVault
appliance at: /etc/openvpn/nodes/[client_IP].tar.gz.
* Copy this configuration file to the remote AlienVault appliance
* Extract the configuration file: /bin/tar xzf [client_IP].tar.gz -C /tmp/
* Move the VPN client configuration file to the OpenVPN folder: cp -arf
/tmp/etc/openvpn/nodes/* /etc/openvpn/; mv /etc/openvpn/[client_IP]/*.conf
/etc/openvpn/
* Fire the configuration triggers: dpkg-trigger --no-await alienvault-network-
vpn-net-client; dpkg --pending --configure
* Clean up: rm -rf /tmp/etc
* Finally, once the VPN connection has been established, please add the remote
AlienVault appliance from the Configuration > Deployment menu option on the
web UI
Press [Enter] to continue
```

This creates a configuration file instead. And you must configure the VPN client manually, as described here.

To configure the VPN client through the command line

1. Transfer the VPN configuration file to the VPN client manually:
 - a. On the VPN server, go to the AlienVault Setup Main menu and select **Jailbreak System**, press **Enter** twice to confirm.
 - b. Go to `/etc/openvpn/nodes/` and locate the `<client_IP>.tar.gz` file, where `<client_IP>` is the VPN client IP address you specified in [step 4 when creating the VPN client](#).
 - c. Using `scp`, or a similarly secure copy method, transfer the `<client_IP>.tar.gz` file to the VPN client and place it in `/etc/alienvault/network/`.
 - d. Type `Exit` to return to the AlienVault Setup main menu.
2. Configuring the tunnel on the VPN client:

- a. SSH to the VPN client.
- b. In the AlienVault Setup menu, select **System Preferences > Configure Network > Setup VPN > Configure VPN client from file**, and press **Enter** (<OK>).
- c. Select the entry with the correct IP address for the VPN client, press **Enter** (<OK>).
- d. Confirm that the configuration file is the correct one, the file copied in Step 3 of this procedure, then press **Enter** (<Yes>).

The system extracts from the configuration file to build a tunnel.

Additional Step When the VPN server and VPN client Reside in Different Networks

Please be aware that if the VPN client and VPN server are in different private networks and the connection from the VPN client to the VPN server is only allowed through their public IP addresses, you need to change the IP address in the configuration file manually.

Let's consider the following example, where the VPN server and VPN client have different private the public IP addresses:

Sample IP addresses for the VPN server and VPN client

	VPN server	VPN client
Private IP	192.168.0.1	172.16.20.56
Public IP	88.132.33.11	145.156.44.33

When configuring the VPN client, enter the public IP address for the client, in this case 145.156.44.33. Extract the resulting `/etc/openvpn/nodes/145.156.44.33.tar.gz` file and locate the VPN client configuration file, `145.156.44.33.conf`. Observe that the private IP address of the VPN server (192.168.0.1) is added instead of the public IP address, as indicated in line 4 below:

```
client
dev tun
proto tcp
remote 192.168.0.1 33800
resolv-retry infinite
nobind
user nobody
group nogroup
verb 3
ca /etc/openvpn/145.156.44.33/ca.crt
cert /etc/openvpn/145.156.44.33/145.156.44.33.crt
```

```
key /etc/openvpn/145.156.44.33/145.156.44.33.key
script-security 2 system
up "/etc/init.d/fprobe stop || true"
comp-lzo
persist-key
persist-tun
```

This causes the VPN tunnel not be established. Changing the IP address to 88.132.33.11 in the file above resolves this issue.

Verifying the VPN Connection

To verify the VPN connection

1. Open a browser window, using the VPN server IP, and log into USM Appliance with administrator credentials.
2. Go to **Configuration > Deployment > Components** and verify that the components display a VPN IP address:

DEPLOYMENT						
ALIENVAULT COMPONENTS INFORMATION						
NAME	STATUS	RAM USAGE	SWAP USAGE	CPU USAGE	NEW UPDATES	
VirtualUSMStandardSensor (IP: 192.168.6.214) VPN IP: 10.67.68.10	UP	29.80 %	0.00 %	0.00 %	[Icons]	
VirtualUSMStandardServer (IP: 192.168.6.20) VPN IP: 10.67.68.11	UP	37.60 %	0.00 %	0.00 %	[Icons]	

This verifies that your VPN connection is intact.

Disabling a VPN Configuration

When you disable a VPN tunnel, it does not remove the configuration files and system-generated certificates from the appliance. You can enable the same tunnel again, if needed.

If you decide instead to establish a new VPN tunnel on the same AlienVault appliance, repeat the procedures. The system then overwrites the existing configurations.

You can disable a VPN configuration from either the VPN server or a VPN client.

To disable a VPN configuration

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 **Configure Network**.
4. Select **Setup VPN**.
5. Select **Enable/Disable VPN**.
6. Use the arrow keys to move to "no", press the spacebar to select, and then press Enter (<OK>).
7. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
8. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

High Availability Configuration

High availability (HA) replicates data to avoid any potential loss of events, assets, or configurations should one or more components cease operation for any reason.

AlienVault strongly recommends that you configure USM Appliance for high availability, particularly, for compliance requirements, so that no data are lost.

**Note:** AlienVaultUSM Appliance supports HA only in its USM Appliance Standard and USM Appliance Enterprise products.

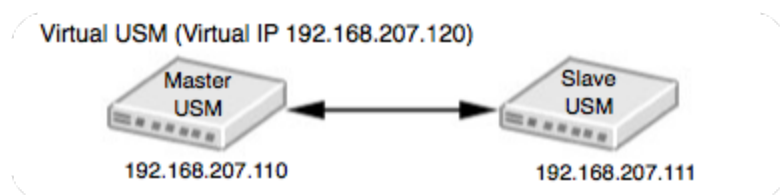
This section covers the following subtopics:

- How Does the High Availability Solution Work?186
- High Availability Prerequisites and Restrictions187
- Configuring High Availability in USM Appliance Standard Systems 189
- Configuring High Availability in USM Appliance Enterprise Systems202
- Disabling High Availability206
- Upgrading a USM Appliance Deployment Configured for High Availability 207

How Does the High Availability Solution Work?

The AlienVaultUSM Appliance high availability solution consists of a set of redundant USM Appliance nodes that mirror each other.

This HA system remains operational, with the primary (master) instance being active and the secondary (slave) instance, passive. If the primary instance fails, the secondary instance becomes active automatically, replacing the failed node.

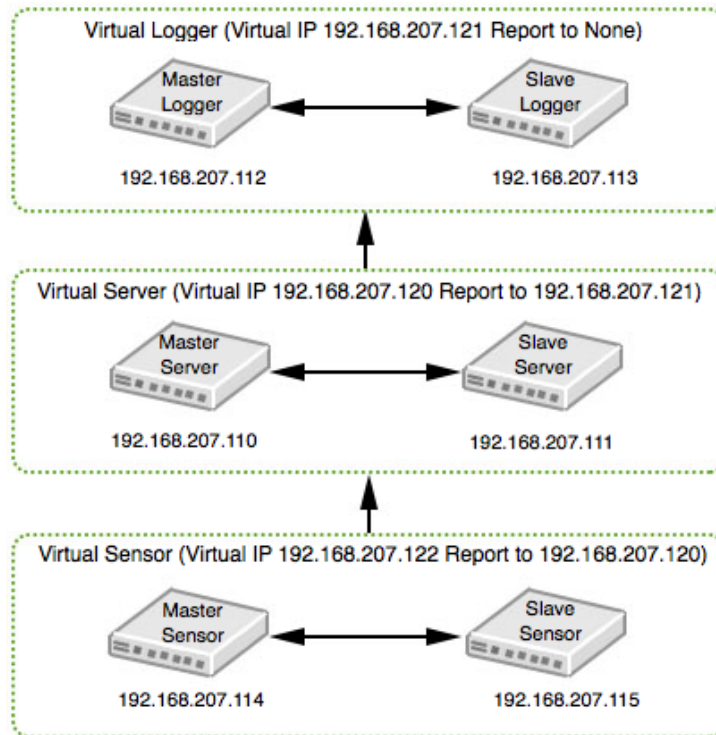


Active (left) and passive (right) nodes for a USM Appliance system component

When you are ready to bring the failed node back on line, it again becomes the active node and the node that took its place reverts to being the passive node. Users must make the switch manually.

Each node has a unique IP address, but shares the same virtual IP address with its clone.

The HA deployment always starts with the USM Appliance Server and the USM Appliance Sensor. If the USM Appliance Logger is part of your USM Appliance deployment, you should configure it last.



Typical HA topology, including loggers

High Availability Prerequisites and Restrictions

Before you start, review the prerequisites and restrictions in setting up a high availability (HA) USM Appliance system.

General Prerequisites and Restrictions

Make sure that you review all of the following AlienVault USM Appliance HA requirements and restrictions carefully before starting your deployment:

- Because this HA feature does not work across dispersed locations (due to their different IP addressing), both the primary and secondary systems must be on the same subnet.
- To avoid any network failures that could affect USM Appliance high availability, nodes must be connected through a dedicated network cable, without any networking equipment.
- Use isolated interfaces (for example, eth1) at each node.

- Make sure that the primary and secondary nodes are running the same image of AlienVault USM Appliance. For example, if the primary node is updated to USM Appliance version 5.3 from a previous version but the secondary node is a fresh install of USM Appliance version 5.3, HA will not work properly.
- When setting up HA in USM Appliance Enterprise systems, the root user password must not contain the following characters: ? * [] { } ! \ ^ \$ " / ' ` < > |

NTP Server Requirements

- Both the primary and secondary nodes require their own dedicated NTP Server. These NTP Servers should be configured identically.
- Both NTP Servers must be up and running, and synchronized with each other.

Configuration Prerequisites — USM Appliance Standard and Enterprise Solutions

These prerequisites and restrictions apply both to the USM Appliance Standard and Enterprise deployments.

- The primary and secondary nodes of a USM Appliance component in an HA deployment cannot share the same hostname.
- You cannot change the IP or hostname of any component in a high availability system once configured.
- You must register both nodes of each component.
- Both the primary and secondary instances must have the same time zone setting.
- Make sure that you configure each node to communicate with the NTP Server for its instance.

Configuration Prerequisites — USM Appliance Enterprise Solution Only

You must configure both nodes for the USM Appliance Enterprise Server and the USM Appliance Enterprise Database with the same root password.

General Maintenance Prerequisites

- Make sure that you always keep the secondary HA instance at parity with the primary USM Appliance instance.
- When upgrading USM Appliance to a new version, HA must be disabled. Otherwise, you lose the HA configuration. You can re-enable HA when the upgrade has finished.



Important: Any network latency or network disconnection issues that can lead to replication failure must be fixed promptly.

Configuring High Availability in USM Appliance Standard Systems

Before You Start

1. Carefully review [High Availability Prerequisites and Restrictions](#).
2. Deploy two instances for each USM Appliance component (USM Appliance Standard Server, USM Appliance Standard Sensor, or, if used, USM Appliance Standard Logger), as described in [USM Appliance Deployments](#).

Configuring High Availability for USM Appliance Standard Servers

The USM Appliance Standard Server is the first USM Appliance component that you must configure for HA.

See also [Example: Configuring High Availability for USM Appliance Standard Servers](#).

You must first deploy and configure the node you intend to act as the passive node, or slave. You configure the active, or master, node, second. Both procedures appear below.

Configuring the Secondary Standard Server for HA

To configure HA in the secondary server

1. Log into the secondary (slave) Standard Server.
2. From the AlienVault Setup Main menu, select **Jailbreak System** and press **Enter** (<OK>).
3. Press **Enter** (<Yes>) to continue.

- When you see the command line prompt, access and edit the file `/etc/ossim/ossim_setup.conf` as indicated in the angle-bracketed variables below:

```
ha_heartbeat_start=yes
ha_local_node_ip=<slave_appliance_IP>
ha_other_node_ip=<master_appliance_IP>
ha_other_node_name=<master_appliance_name>
ha_password=<password>
**This password must be the same for both slave and master.**
ha_role=slave
ha_virtual_ip=<virtual_IP>
```



Important: The `ha_role` value must always equal "slave" for the secondary node.

- Save the changes.
- Enable HA in the slave by entering the following command:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

- Check that the secondary node is up and running by entering:

```
alienvault-ha-assistant -s
```

- When prompted, enter the remote (master) root user password.

After about five minutes, you see the following output:

```
Please, we need the remote root user password
Password:
HA Status
-----
Node Name: haslave (local)
Node IP   : 192.168.212.16
Heartbeat status: Running
Resources: all
-----
Node Name: hamaster
Node IP   : 192.168.212.15
Heartbeat status: unknown
Resources: undefined
-----
haslave:~#
```

Configuring the Primary Standard Server for HA

To configure HA in the primary server

1. Log into the primary (master) Standard Server.
2. From the AlienVault Setup Main menu, select **Jailbreak System** and press **Enter** (<OK>).
3. Press **Enter** (<Yes>) to continue.
4. When you see the command line prompt, access the file `/etc/ossim/ossim_setup.conf` and edit it as indicated within the angle-bracketed variables, as shown below:

```
ha_heartbeat_start=yes
ha_local_node_ip=<master_appliance_IP>
ha_other_node_ip=<slave_appliance_IP>
ha_other_node_name=<slave_appliance_name>
ha_password=<password>
**This password must be the same for both slave and master.**
ha_role=master
ha_virtual_ip=<virtual_IP>
```

5. Save the changes.
6. Enable HA in the primary (master) node:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

This outputs the following:

```
INFO: Updating firewall configuration...
INFO: Restarting rsync...
INFO: Enable mysql replication
INFO: database info updated
INFO: database tables updated
INFO: Force slave to release resources...
INFO: Checking cron entries...
INFO: restarting service cron
Success!!!!!!
You have new mail in /var/mail/root
Hostname1:~#
```

7. Check that the primary node is up and running:

```
alienvault-ha-assistant -s
```

8. When prompted, enter the remote (slave) root user password.

After about five minutes, you see output confirming that the node is running.

9. Launch a web browser and verify that you can access the USM Appliance system, using the HA virtual IP specified in the `ossim_setup.conf` file.

Example: Configuring High Availability for USM Appliance Standard Servers

This topic provides an example of how to configure two USM Appliance Standard Servers in a high availability environment.

This configuration uses the following IP addresses:

- Master: 192.168.7.235 (MasterAppliance)
- Slave: 192.168.7.254 (SlaveAppliance)
- Virtual IP: 192.168.7.236

The primary appliance has the name *MasterAppliance*, and the secondary appliance has the name *SlaveAppliance*.



Important: Do not use spaces in the appliance names!

To deploy two high availability Standard Servers

1. If not already done, deploy the USM Appliance Standard Server according to the instructions in [USM Appliance Deployments](#).
2. Change the root user password in both appliances, as described in "Reset Password for the Root User" in the *USM Appliance User Guide*, making sure that the password is the same in each.
3. Configure the hostname in the master (primary) appliance:
 - a. On the AlienVault Setup Main menu, go to **System Preferences > Configure Host-name**.
 - b. Enter the hostname for the primary component:


```
MasterAppliance
```
 - c. Press **Enter** (<OK>).
4. Configure the hostname in the slave (secondary) appliance:

a. Go to **System Preferences > Configure Hostname**.

b. Enter the hostname for the secondary component:

```
SlaveAppliance
```

c. Press **Enter** (<OK>).

5. Configure each failover pair to communicate and synchronize with its respective NTP server.

See [High Availability Prerequisites and Restrictions](#) and [Configure Synchronization with an NTP Server](#).

6. Restart both appliances.

7. On the secondary (slave) appliance, launch the AlienVault console.

8. On the AlienVault Setup Main menu, choose **Jailbreak System**.

9. When you see the command line prompt, edit the file `/etc/ossim/ossim_setup.conf` as below

```
[ha]
ha_autofailback=no
ha_deadtime=10
ha_device=eth0
ha_heartbeat_comm=bcast
ha_heartbeat_start=yes
ha_keepalive=3
ha_local_node_ip=192.168.7.254
ha_log=no
ha_other_node_ip=192.168.7.235
ha_other_node_name=hostname1
ha_password=temporal
ha_ping_node=default
ha_role=slave
ha_virtual_ip=192.168.7.236
```

10. Save the changes.

11. Enable HA in the secondary node by entering:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

12. Check that the secondary node is up and running:

```
alienvault-ha-assistant -s
```

13. When prompted, enter the root user password for the primary (master) server.

After about five minutes, you see output, showing HA status for the secondary (slave) heartbeat status should be `Running`.

14. On the primary (master) appliance, log into the AlienVault console.
15. On the AlienVault Setup Main menu, choose **Jailbreak System**.
16. Edit the `/etc/ossim/ossim_setup.conf` file as below

```
[ha]
ha_autofailback=no
ha_deadtime=10
ha_device=eth0
ha_heartbeat_comm=bcast
ha_heartbeat_start=yes
ha_keepalive=3
ha_local_node_ip=192.168.7.235
ha_log=no
ha_other_node_ip=192.168.7.254
ha_other_node_name=hostname2
ha_password=temporal
ha_ping_node=default
ha_role=master
ha_virtual_ip=192.168.7.236
```

17. Save the changes.
18. Enable HA in the primary node:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

19. Verify that the primary node is up and running:

```
alienvault-ha-assistant -s
```

20. When prompted, enter the root user password for the secondary server.

After about five minutes, you see output, showing HA status for the secondary (slave) heartbeat status as Running.

21. Launch a web browser, check that you can access the USM Appliance Standard Server through the `ha_virtual_ip` assigned in the `ossim_setup.conf` file.

It should look like the following:

The screenshot shows the AlienVault Center web interface. The top navigation bar includes 'DEPLOYMENT' and tabs for 'COMPONENTS', 'SCHEDULER', 'SMART EVENT COLLECTION', and 'LOCATIONS'. Below this, there are links for 'ALIENVAULT CENTER', 'SENSORS', 'SERVERS', and 'REMOTE INTERFACES'. The main content area is titled 'ALIENVAULT COMPONENTS INFORMATION' and contains a table with the following data:

NAME	STATUS	RAM USAGE	SWAP USAGE	CPU USAGE	NEW UPDATES
Hostname1 [192.168.7.235] Server Sensor Web Interface Database	UP [Active HA]	84.60 %	3.70 %	0.00 %	Download icon
Hostname2 [192.168.7.254] Server Sensor Web Interface Database	UP [Passive HA]	20.20 %	0.00 %	0.00 %	Download icon

At the bottom of the table, it says 'SHOWING 1 TO 2 OF 2 ENTRIES' and 'FIRST PREVIOUS 1 NEXT LAST'.

Configuring High Availability for USM Appliance Standard Sensors

This process has three tasks you perform in the following order:

- [Configuring the Secondary Standard Sensor for HA](#)
- [Configuring the Primary Standard Sensor for HA](#)
- [Configuring Communication Between the Standard Sensors and the Standard Servers](#)

Configuring the Secondary Standard Sensor for HA

To configure a secondary sensor in HA

1. Log into the secondary Standard Sensor.
2. From the AlienVault Setup Main menu, select **Jailbreak System** and press **Enter** (<OK>).
3. Press **Enter** (<Yes>) to continue.

The command line prompt appears.

4. Configure the secondary (slave) sensor:

- a. Edit the file `/etc/ossim/ossim_setup.conf` as indicated by the angle-bracketed variables:

```
ha_heartbeat_start=yes
ha_local_node_ip=<slave_appliance_IP>
ha_other_node_ip=<master_appliance_IP>
ha_other_node_name=<master_appliance_name>
ha_password=<password>
**Password must be same for both slave and master**
ha_role=slave
ha_virtual_ip=<virtual_appliance_IP>
```



Important: The `ha_role` value must always equal "slave" for the secondary node.

- b. Save the changes.

5. Enable HA in the secondary node:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

6. Check that the secondary node is up and running

```
alienvault-ha-assistant -s
```

7. When prompted, enter the password for the primary (master) root user.

You must wait about five minutes until you see output, as shown in Step 8 of [Configuring the Secondary Standard Server for HA](#).

Configuring the Primary Standard Sensor for HA

To configure the primary sensor for HA

1. From the primary Standard Sensor, access the file `/etc/ossim/ossim_setup.conf`, as described in [Configuring the Secondary Standard Sensor for HA](#).
2. Change its fields as indicated below:

```
ha_heartbeat_start=yes
ha_local_node_ip=<primary_appliance_IP>
ha_other_node_ip=<secondary_appliance_IP>
ha_other_node_name=<secondary_appliance_name>
ha_password=<password>
**Password must be same for both secondary and primary (master)**
ha_role=master
```



```
ha_virtual_ip=<virtual_appliance_IP>
```

3. Save the changes.
4. Enable HA in the primary (master) node by typing the following command:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

5. Swap the token with the secondary node, effectively making the primary node active:

```
alienvault-ha-assistant -w
```

6. Check that the primary node is up and running:

```
alienvault-ha-assistant -s
```

7. When prompted, enter the remote (slave) root user password.

After about five minutes, you see output, as shown in Step 8 of [Configuring the Secondary Standard Server for HA](#)

Configuring Communication Between the Standard Sensors and the Standard Servers

You configure communication between servers and sensors in the following order:

- First: Primary sensor to primary server
- Second: Secondary sensor to primary server
- Third: Primary sensor and secondary server
- Fourth: Secondary sensor and secondary server

Configuring Communication Between the Primary Sensor and the Primary Server

To configure communication between the primary sensor and the primary server

1. Log into the primary Standard Sensor.



Note: If you are still logged into the appliance from the previous task and in command line mode, return to the Setup Main menu by entering `alienvault-setup`.

2. From the AlienVault Setup Main menu, select **Configure Sensor > Configure AlienVault Server IP**.

3. Enter the virtual IP address of the USM Appliance Standard Server pair and press **Enter** (<OK>).
4. Select **Configure AlienVault Framework IP**, then enter the same IP address; press **Enter** (<OK>).
5. Launch the AlienVault USM Appliance web interface and go to **Configuration > Deployment > Components > Sensors**.
6. Insert the primary USM Appliance Standard Sensor.

Configuring Communication Between the Secondary Sensor and the Primary Server

This task uses the AlienVault console exclusively.

To add the secondary sensor to the primary server

1. Log into the primary Standard Server and select **Jailbreak System**, press **Enter** (<OK>), and again **Enter** (<Yes>).
2. At the command prompt, enter the following:

```
alienvault-api add_system --system-ip=<secondary_std_sensor_ip> --
password=<password> --ha
```

Configuring Communication Between the Primary Sensor and the Secondary Server

To add the primary sensor to the secondary server

1. Log into the secondary Standard Server, repeat step 1. (jailbreak the system) of the previous task.
2. At the command prompt, enter the following:

```
alienvault-api add_system --system-ip=<primary_std_sensor_ip> --
password=<password> --ha
```

Configuring Communication Between the Secondary Sensor and the Secondary Standard Server

To add the secondary sensor to the secondary server

1. On the secondary Standard Server, repeat step 1. (jailbreak the system) of the previous task.
2. At the command prompt, enter the following:

```
alienvault-api add_system --system-ip=<secondary_std_sensor_ip> --
password=<password> --ha
```

Duplicating Firewall Rules in USM Appliance Standard Sensors

Whenever you add one or more USM Appliance Standard Sensors to the USM Appliance Standard Server in a system, you must add server-specific firewall rules to the sensors. This preserves the ability to execute remote scans.

This topic describes how to add firewall rules and also how to disable them when you need to disable HA, for example, during an upgrade.

Adding Server-Specific Firewall Rules to Sensors

To add server-specific firewall rules to the sensors

- On each USM Appliance Standard Sensor, enter the following command, even if not all sensors are part of the HA configuration:

```
alienvault-ha-assistant -f <master_server_ip> <slave_server_ip>
```

Removing Firewall Rules from Sensors

To remove firewall rules from sensors when HA has been disabled in the servers

- Run the following command in the USM Appliance Standard Sensor(s) to remove the configuration:

```
alienvault-ha-assistant -d
```

Restoring Firewall Rules in Sensors

When you disable an HA connection between two USM Appliance Standard Sensors at the same level, it disables all HA firewall rules, not only in that location, but also among sensors at the upper level. For this reason, you must restore the firewall configuration after any HA disablement.

To restore the firewall configuration on the sensors

- Run the following command in the USM Appliance Standard Sensor(s) to restore firewall rules:

```
alienvault-ha-assistant -f <master_server_ip> <slave_server_ip>
```

Configuring High Availability for USM Appliance Standard Loggers

Prerequisites

- You must have already deployed and configured the USM Appliance Standard Logger as described in [USM Appliance Deployments](#) minus the task of [Configure the USM Appliance Logger after Deployment](#).
- You must have already configured the USM Appliance Standard Servers for HA.
- You may configure the USM Appliance Standard Loggers for HA either before or after the USM Appliance Standard Sensors.

Configuring the Secondary Logger for HA

To configure a secondary logger for HA

1. Log into the secondary Standard Logger.
2. From the AlienVault Setup Main menu, select **Jailbreak System**, press **Enter** (<OK>), and **Enter** again.
3. After you see the prompt, configure HA in the secondary node, or slave in `/etc/ossim/ossim_setup.conf` as indicated by the angle-bracketed text:

```
ha_heartbeat_start=yes
ha_local_node_ip=<slave_appliance_IP>
ha_other_node_ip=<master_appliance_IP>
ha_other_node_name=<master_appliance_name>
ha_password=<password>
**The password for both slave and master must be the same.**
ha_role=slave
ha_virtual_ip=<virtual_appliance_IP>
```



Important: The `ha_role` value must always equal "slave" for the secondary node.

4. Save the changes.
5. Enable HA in the secondary node by entering the following command:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

6. Check that the secondary node is up and running by entering:

```
alienvault-ha-assistant -s
```

7. When prompted, enter the remote (master) user password.

After about five minutes, you see output, as shown in Step 8 of [Configuring the Secondary Standard Server for HA](#).

Configuring the Primary Logger for HA

To configure the primary logger for HA

1. Follow steps 1. through 3. in [Configuring the Secondary Logger for HA](#).
2. Edit the file `/etc/ossim/ossim_setup.conf` as indicated:

```
ha_heartbeat_start=yes
ha_local_node_ip=<master_appliance_IP>
ha_other_node_ip=<slave_appliance_IP>
ha_other_node_name=<slave_appliance_name>
ha_password=<password>

**This password must be the same for both slave and master.**

ha_role=master
ha_virtual_ip=<virtual_appliance_IP>
```

3. Save the changes.
4. Enable HA in the primary node by entering the following:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

5. Check that the primary node is up and running:

```
alienvault-ha-assistant -s
```

6. When prompted, enter the remote (slave) root user password.

After about five minutes, you see output.

7. Launch a web browser and verify that you can access the USM Appliance system, using the virtual IP specified in the `ossim_setup.conf` file.

Configuring Communication Between the Loggers and Servers

You must add the primary Standard Server to the primary Standard Logger through the web interface.

You configure communication between the remaining nodes solely through the AlienVault console.

Adding the Primary Server to the Primary Logger

See [Configure the USM Appliance Logger after Deployment](#).

Adding the Secondary Server to the Primary Logger

Complete this task only **after** you have added the primary Standard Server to the primary (active) logger through the USM Appliance web interface.

To add the secondary server to the primary logger

1. Log into the primary Standard Logger.
2. From the AlienVault Setup Main menu, select **Jailbreak System**.
3. From the command prompt, add the secondary Standard Server:

```
alienvault-api add_system --system-ip=<secondary_std_server_ip> --
password=<USM_root_password> --ha
```

Adding the Primary Server to the Secondary Logger**To add the primary server to the secondary logger**

1. Log into the secondary Standard Logger.
2. Repeat steps 2. and 3. of [Adding the Secondary Server to the Primary Logger](#).

```
alienvault-api add_system --system-ip=<primary_std_server_ip> --
password=<USM_root_password> --ha
```



Note: Keep the session open and in command line mode for completion of the next task.

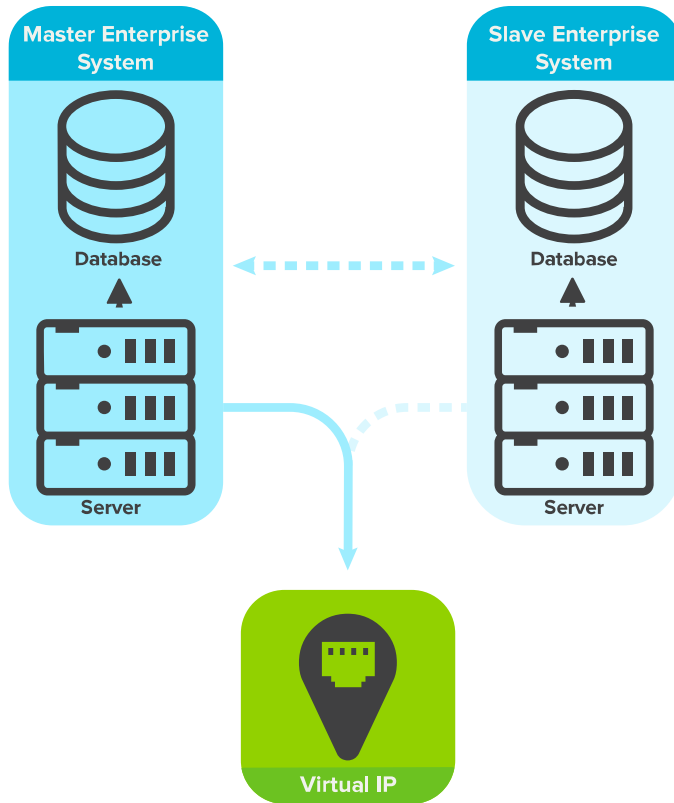
Adding the Secondary Server to the Secondary Logger**To add the secondary server to the secondary logger**

- From the command line of the secondary Standard Logger, add the secondary Standard Server:

```
alienvault-api add_system --system-ip=<secondary_std_server_ip> --
password=<USM_root_password> --ha
```

Configuring High Availability in USM Appliance Enterprise Systems


Unlike the USM Appliance Standard Server topology, the USM Appliance Enterprise Server consists of two separate devices, an Enterprise Server and an Enterprise Database. Configuration consists of configuring the Enterprise Servers to communicate with their Enterprise Databases, and for one Enterprise Server to fail over to another.



USM Appliance Enterprise Server and Database in an HA topology

Prerequisites

- You must have already deployed and configured each appliance, as described in [Configure the USM Appliance Hardware](#).
- You must have configured the following:
 - The same root password in both the Enterprise Server and Enterprise Database.

 **Important:** When setting up HA in USM Appliance Enterprise systems, the root user password must not contain the following characters: ? * [] { } ! \ ^ \$ " / ' ` < > |

- A hostname for each failover node pair that makes it obvious which is the master and

which the slave.

- Communication and synchronization with the respective NTP servers for each failover node.

Configuring HA in the Secondary Enterprise Server and Database

To configure HA in the secondary USM Appliance Enterprise Server and Database

1. Log into the secondary Enterprise Server, jailbreak the console, and set HA values, as described in [Configuring High Availability for USM Appliance Standard Servers](#).
2. Configure the secondary Enterprise Database:
 - a. Log into the Enterprise Database node intended for the secondary Enterprise Server node and jailbreak the console.
 - b. At the command line prompt, configure HA by editing the file `/etc/ossim/ossim_setup.conf`, as indicated in the angle-bracketed variables:

```
ha_heartbeat_start=yes
ha_local_node_ip=<slave_database_admin_IP>
ha_other_node_ip=<master_database_admin_IP>
ha_role=slave
```

- c. Save the changes.
3. Log back into the secondary Enterprise Server node and jailbreak the console.
4. At the command line prompt, enter:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

5. Check that the secondary node is up and running by executing:

```
alienvault-ha-assistant -s
```

The system prompts you for the primary (master) *root user* password.

6. Enter the password, then wait approximately five minutes until a screen appears, showing a value of `Heartbeat status=Running`.

Configuring HA in the Primary Enterprise Server and Database

To configure HA in the primary Enterprise Server and Database

1. Follow the steps in [Configuring HA in the Secondary Enterprise Server and Database](#), but in `/etc/ossim/ossim_setup.conf`, make the changes shown in the angle-bracketed variables below:

```
ha_heartbeat_start=yes
ha_local_node_ip=<master_database_admin_IP>
ha_other_node_ip=<slave_database_admin_IP>
ha_role=master
```

2. Save the changes.
3. Log into the primary, or master, Enterprise Server, jailbreak the console, and, at the command line prompt, enter:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

Adding an Enterprise Database to an Enterprise Server

You must add

- The primary Enterprise Database to the secondary Enterprise Server node.
- The secondary Enterprise Database to the primary Enterprise Server node.

To add the Enterprise Database to an Enterprise Server

1. Log into the secondary Enterprise Server.
2. Select **Jailbreak System**, press **Enter** (<OK>), and **Enter** (<Yes>) again.
3. Add the *primary* Enterprise Database to the secondary Enterprise Server node, using the command:

```
alienvault-api add_system --system-ip=<master_database_admin_ip>
--password=<root_password_to_master_database>
```

4. Log into the primary Enterprise Server node as previously described, and add the *secondary* Enterprise Database:

```
alienvault-api add_system --system-ip=<slave_database_admin_ip>
--password=<root_password_to_slave_database>
```

Verifying the Configuration

To check the configuration

1. Using the virtual IP address referenced in `ossim-setup.conf`, launch the USM Appliance web interface in a browser.
2. Go to **Configuration > Deployment > Components > AlienVault Center**.

Both databases should be visible, including the one functioning as a secondary, or slave, database.

NAME	STATUS	RAM USAGE	SWAP USAGE	CPU USAGE	NEW UPDATES
anadatabase [192.168.6.151] Server Sensor Web Interface Database	UP	8.40 %	0.00 %	0.00 %	--
anaserver [192.168.6.134] Server Sensor Web Interface Database	UP [Passive HA]	5.40 %	0.00 %	0.00 %	--
USMEnterpriseDatabase [192.168.6.83] Server Sensor Web Interface Database	UP	4.90 %	0.00 %	5.88 %	--
USMEnterpriseServer [192.168.6.84] Server Sensor Web Interface Database	UP [Active HA]	9.10 %	0.00 %	0.00 %	--

SHOWING 1 TO 4 OF 4 ENTRIES

FIRST PREVIOUS 1 NEXT LAST

Disabling High Availability

About Disabling HA in Network Nodes

You must disable HA components in the following order:

USM Appliance Standard	USM Appliance Enterprise
1. Logger pair	1. Logger pair
2. Server pair	2. Server pair
3. Sensor pair	3. Database pair
	4. Sensor pair

About Disabling HA in Components Not Configured for It

If you have any USM Appliance Standard or Enterprise Sensors that you **did not** configure for HA, you must still run the HA disablement command on them after you disable HA in the USM Appliance Standard or Enterprise Server pair. This removes any firewall rules created when HA was configured.



Important: If you fail to do this, you can introduce a vulnerability into the network.

Disabling HA in a Failover Pair

To disable HA in a failover pair

1. Log into the secondary (slave) node and launch the AlienVault console.
2. In the AlienVault Setup Main menu, select **Jailbreak System**, press **Enter** (<OK>), then **Enter** (<Yes>) again.
3. From the command line prompt, disable HA:

```
alienvault-ha-assistant -d
```

4. Exit the command line mode:

```
exit
```

5. In the primary (master) node, repeat steps 1. through 4.

6. Exit the command line mode:

```
exit
```

7. Repeat the foregoing steps for all of the component pairs in your HA deployment the previously mentioned order.

Upgrading a USM Appliance Deployment Configured for High Availability

Prerequisites

To upgrade USM Appliance to a new version, you must first temporarily disable HA. See [Disabling High Availability](#).

Order of Component Upgrade

You must upgrade USM Appliance Standard or Enterprise components in the following order, starting with the secondary and moving to the primary node:

- Loggers
- Servers
- Sensors

Upgrading USM Appliance

To upgrade USM Appliance

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

The AlienVault Setup menu displays.

2. Update the node by selecting **System Preferences > Update AlienVault System > Update System**.

3. Press **Enter** (<Yes>) and wait until you see the following message:

```
Your system has been updated successfully
```

4. Press **Enter** (<OK>).
5. 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.
6. Edit `/etc/ossim/ossim_setup.conf` and set `ha_heartbeat_start=yes`.



Note: You need to do this step because `ha_heartbeat_start` was set to `no` when disabling HA before the update.

7. Repeat steps #1 through #6 on the **primary** node.
8. Re-enable HA.

Run this command first on the secondary node, then on the primary node:

```
screen alienvault-ha-assistant -e
```



Note: Use `screen` to keep the process running in the background even when the session disconnects.

9. (If and only if upgrading the **Standard Sensors**) On the primary node, swap the token with the secondary node, effectively making the primary node active:

```
alienvault-ha-assistant -w
```

Plugin Management

The USM Appliance plugins provide logic to extract security-specific data from external applications and devices to produce events managed by the USM Appliance Server. USM Appliance comes equipped with plugins for many commonly encountered data sources that you can select and enable for specific assets to start collecting data. For a list of all the plugins that USM Appliance supports, see the [USM Appliance Supported Plugins](#) list.

AlienVault provides more than one way to enable plugins in USM Appliance. You can enable plugins on specific discovered assets, or you can enable plugins globally on USM Appliance Sensors. In addition, based on the plugin types, you can enable plugins using different tools, including the USM Appliance web UI, the Getting Started Wizard, or the AlienVault Console.

Most of the plugins in USM Appliance do not require additional configuration after they are enabled, especially if you enable the plugin on an asset. But if you choose to enable the plugin at the sensor level and USM Appliance does not have the required configuration files on the sensor; or if you are enabling a database plugin, an SDEE plugin, or a WMI plugin, you will need to perform some extra steps before the plugin can operate correctly.

In a limited number of environments, the built-in plugins may not quite fit specific needs or provide enough intelligence to normalize data and extract required information from all logs received. In such cases, you may be able to customize an existing plugin. You can also create your own custom plugins, choosing from various options available to create plugins by scratch, and directly editing plugin configuration file; or use the plugin builder provided in the USM Appliance web UI, to create a plugin using an interactive program wizard.

Topics covered in this section include

Plugin Fundamentals	.211
Enable Plugins	.227
Configure Plugins	.237
Customize and Develop New Plugins	.258

Plugin Fundamentals

The USM Appliance Sensor uses plugins to extract and normalize data received from different data sources.



Note: You can examine which data sources are supported by default by examining the content of the `/etc/ossim/agent/plugins` directory, or by examining listed data sources in the AlienVault Console or in the USM Appliance web UI.

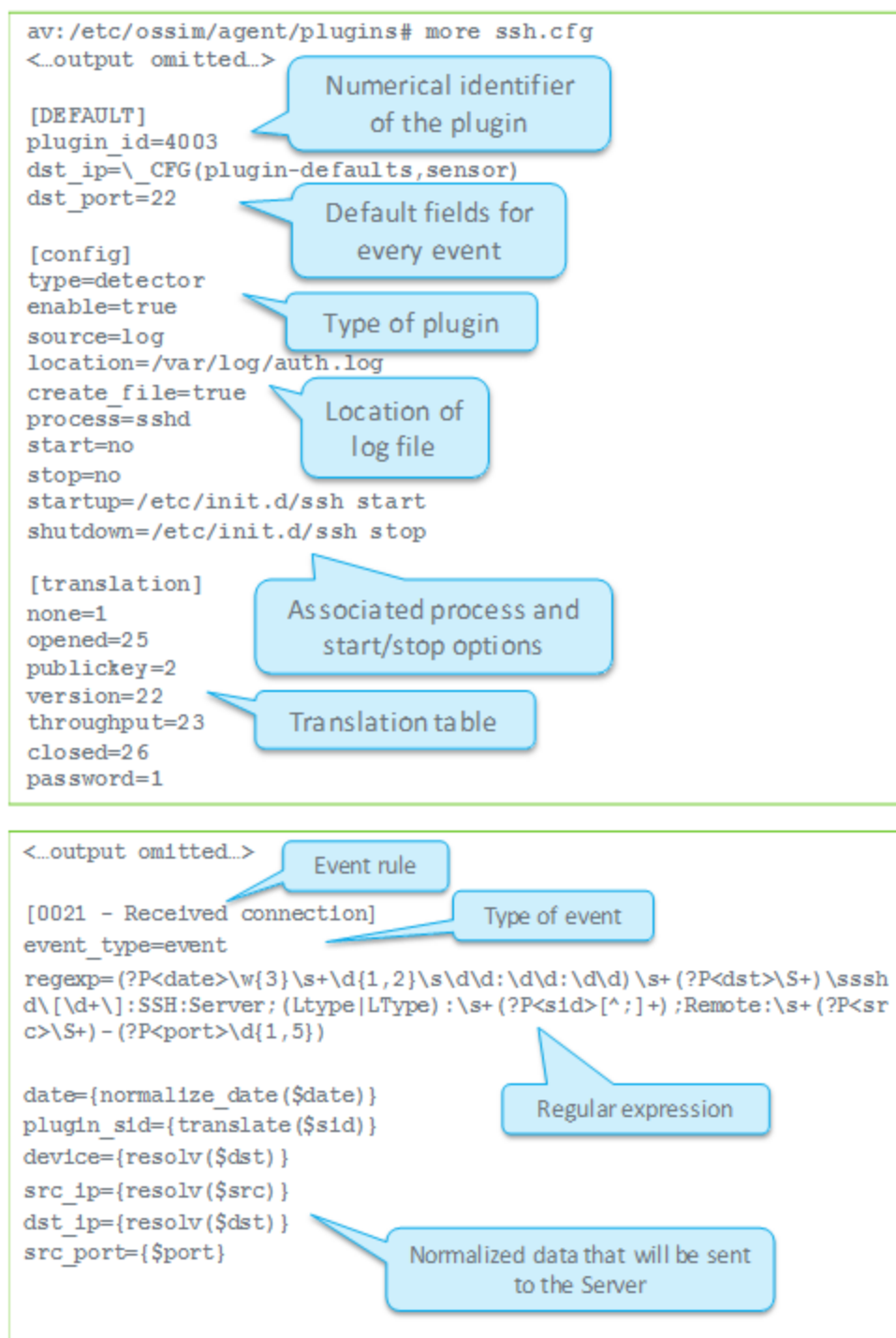
During data normalization, a plugin evaluates each log file line and translates it to an event that identifies the event's type and subtype within the USM Appliance Event Taxonomy.

Each USM Appliance plugin include two files

- **<plugin_name>.cfg** — Resides on each USM Appliance Sensor under `/etc/ossim/agent/plugins`. This file specifies the plugin configuration parameters, and the rules a log line must match before USM Appliance collects and normalizes them.
- **<plugin_name>.sql** — Resides on the USM Appliance Server under `/usr/share/doc/ossim-mysql/contrib/plugins`. This file describes every event, and the corresponding event fields, that the plugin may store in the SIEM database for events extracted from a data source.

Plugin Configuration File Structure

The following figure shows an example of the `.cfg` data source plugin file. The file shown in this example enables the USM Appliance Sensor to parse SSH events.



The plugin configuration file consists of several sections.

The Plugin File Header — lead-in section that provides basic information on relevant vendor, product, version, and per asset information associated with a plugin.

The DEFAULT Section — Provides plugin ID and default values of fields for every event parsed by the plugin. In the example, default values are set for the destination IP address and destination port.

The Config Section — Defines the plugin type, whether a plugin is enabled, source of the plugin, location of a log file the plugin is reading from, and associated processes and start and stop functions.

The Translation Section — Provides translation and conversion of extracted log token and other text and numeric data to values stored in the SIEM database.

The Rules Section — Used to define one rule for each event that may come from a data source. Each rule is composed of a regular expression that defines how to extract information from log events, and mapping between extracted information and the normalized event fields. In the example, only one rule is shown on the right side of the slide for the sake of readability.

The Plugin File Header

All plugin configuration files must include a header.

```
# Plugin {{ plugin_name }} id:{{ plugin_id }} version: -
# Last modification: {{ LAST_MODIFICATION_DATE }}
#
# Plugin Selection Info:
# {{vendor}}:{{model}}:{{version}}:{{per_asset}}
#
# END-HEADER
#
# Accepted products:
#
# Description
```

The `Plugin Selection Info` section includes relevant vendor, product, version, and per asset information.

- **Product and Vendor Information** — Express the product name and vendor information for the plugin, using the following format: `Fortinet:Fortigate`. In this example, Fortigate is the product and Fortinet is the vendor of that product.
- **Version Information** — The version information allows you to select the right plugin when multiple plugins exist for any one version, or when there are multiple plugins, based on log format or intended output.

All plugins set version information to "-" out of the box, because not all applications use versions. Should this be the case for your plugin, you can just maintain the default setting of the version field. When customizing or creating new plugins, verify whether or not your plugin is versioned and, if so, add the version information.

- **Per Asset Information** — Some plugins must be activated for each asset in your network. If `Per Assets` is not set, USM Appliance defaults to "Yes" (Y) and activates the plugin on each asset.

If your plugin should **not** be activated per asset (the AlienVault HIDS plugin, for example), `Per Asset` must read "No" (N).

The DEFAULT Section

The [DEFAULT] section of the plugin configuration file specifies the `plugin_id`, which is a unique ID for the plugin data source. For example, `plugin_id=4003` is a plugin for OpenSSH. The plugin ID is also used when referring to plugins in correlation rules, and when defining policies in USM Appliance.

Users can use the range of 9001 to 2147483647 as plugin IDs, except for the following values, which are reserved

90003, 90005, 90007, 90008, 10002, 12001, 19004, 19005, 19006, 20505

The Config Section

The [config] section of the plugin configuration file specifies the basic settings for this plugin. For example

- `type` — specifies the plugin type, detector, for example.
- `enable` — specifies whether the plugin is enabled or not.
- `source` — identifies the plugin source, using the following keywords
 - `log` — Text log file (for example: SSH, Apache)
 - `mssql` — Microsoft SQL Server database (for example: panda-se)
 - `mysql` — MySQL database (for example: moodle)
 - `wmi` — Windows Management Instrumentation (wmi-system-logger)
- `location` — specifies the name and location of the log file the plugin is reading from, for example, `location=/var/log/file.log`. The rsyslog rules define the location of log files used to store incoming logs from different data sources.



Note: Location is present only in plugins that use a log as a source. Plugins that use other sources contain other plugin-specific information (for example, how to connect to a MySQL database).

The Translation Section

The [translation] section translate token values of a source log and assign them to a normalized event field. Translations are useful when you have similar log messages that describe different events, such as when the difference between messages is only in the value of a token and not the structure of the message itself. In this situation, you can use only one rule to parse different messages and use translations to translate (non-numeric) values from messages to numeric values that can be used as plugin_sid (event type ID) values.

Translations consist of two parts

- **Translation table** — Defines the mapping between values in log messages and values in normalized event.
- **translate() function** — Translates values from tokens into values in normalized event fields by following the translation table.

In the sample configuration file (shown in the `ssh.cfg` illustration), the “sid” token in the log message can take the following non-numeric values: none, opened, publickey, version, throughput, closed, and password. Different values of the sid token indicate different log messages. Values of the sid token are translated into numeric values as defined by the translation table, and then used as the plugin_sid value for individual events. Translations can also be defined to convert other text values to numbers as well.

```
[translation]
none=1
opened=25
publickey=2
version=22
throughput=23
closed=26
password=1
```

```
[0021 - Received connection]
event_type=event
regexp=(?P<date>\w{3}\s\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<dst>\S+)\s+sshd\[\d+\]: SSH: Server; (Ltype|LType):\s+(?P<sid>[^;]+);Remote:\s+(?P<src>\S+) - (?P<port>\d{1,5})
date={normalize_date($date)}
plugin_sid={translate($sid)}
device={resolve($dst)}
src_ip={resolve($src)}
dst_ip={resolve($dst)}
src_port={$port}
```

The Rules Section

The rest of the plugin configuration file belongs to the rules section. It contains rules that define the format of each event and how data extracted by a regular expression for each event will be normalized into standard event fields. Each rule in a plugin is defined with a name and the event type, which is defined using the `event_type=event` line in the plugin configuration file.

The `regexp` field contains the regular expression that defines the format of the events, and extracts the information to normalize it. The regular expressions are written using Python regular expression syntax.

```
[0000 - Failed password]
event_type=event
regexp=(?P<date>\w{3}\s+\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<dst>\S+) sshd\[\d+\]:
Failed password for\s(?P<info>invalid user\s)?(?P<user>\S+)\sfrom\s
(?P<src>\S+)\sport\s(?P<sport>\d{1,5})
date={normalize_date($date)}
plugin_sid=1src_ip={resolve($src)}
dst_ip={resolve($dst)}src_port={$sport}
username={$user}
userdata1={$info}
userdata2={$dst}
device={resolve($dst)}
```



Note: For more information about the syntax or construction of regular expressions, refer to resources on the subject available on the Internet. You may also want to check out AlienVault® Training courses that provide more information and hands-on labs covering plugin development and, in particular, regular expressions used to define plugin rules.

Event Database Field Mapping

In addition to the regular expression, each rule must specify how to map extracted information from a log into a normalized SIEM database event. The following figure shows the event fields into which you can map information extracted from a log using the regular expression defined for a specific rule.

<i>plugin_id</i> ★	<i>plugin_sid</i> ★	<i>date</i> ♦	<i>sensor</i> ♦	<i>interface</i> ♦	<i>protocol</i> ♦
<i>src_ip</i> ♦	<i>src_port</i> ♦	<i>dst_ip</i> ♦	<i>dst_port</i> ♦	username ○	password ○
filename ○	userdata1 ○	userdata2 ○	userdata3 ○	userdata4 ○	userdata5 ○
userdata6 ○	userdata7 ○	userdata8 ○	userdata9 ○		

In the figure

- Fields that are shown in italics are mandatory in each normalized event.
- Fields that are shown in blue (★) include values that always have to be defined in the plugin file.
- Fields that are shown in green (♦) include values that will be filled automatically in case the values are not found in the log (for example, source IP address is set to 0.0.0.0, and source and destination ports are set to 0, if not found in the log).
- Fields that are shown in grey (○) are optional and can be left empty if the values are not found in the log.

Order of Rules Processing

Plugin rules are loaded in sequential order and the rule name of the plugin file is mandatory. Once a log matches one of the regular expressions of one rule, the USM Appliance Sensor stops processing the event.

It is recommended that specific rules be defined with a low numerical value in the name and general rules be defined with a large numerical value in the name. Naming specific rules with lower values allows them to be processed before the general rules, which are defined to catch all events that were not previously matched.

For example

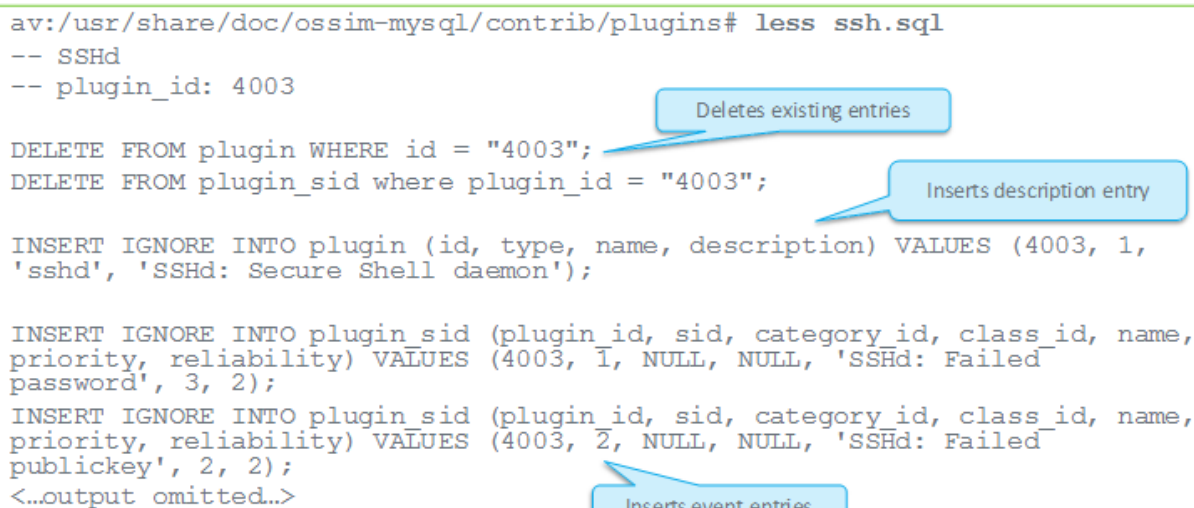
```
[0001 - Specific rule]
[0002 - Specific rule]
[9999 - General rule]
```

Plugin .SQL Files

The .SQL file associated with a plugin defines all database entries inserted by events extracted from the plugin source data or log file.

- Plugin ID
- Event type ID
- Database fields written for each event
- Name assigned to the event
- Priority and reliability values

The following illustration shows the `ssh.sql` file associated with the `ssh.cfg` file described in previous sections.



```

av:/usr/share/doc/ossim-mysql/contrib/plugins# less ssh.sql
-- SSHd
-- plugin_id: 4003

DELETE FROM plugin WHERE id = "4003";
DELETE FROM plugin_sid where plugin_id = "4003";

INSERT IGNORE INTO plugin (id, type, name, description) VALUES (4003, 1,
'sshd', 'SSHd: Secure Shell daemon');

INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority, reliability) VALUES (4003, 1, NULL, NULL, 'SSHd: Failed
password', 3, 2);
INSERT IGNORE INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority, reliability) VALUES (4003, 2, NULL, NULL, 'SSHd: Failed
publickey', 2, 2);
<...output omitted...

```

If you have , you need to import the corresponding plugin.sql file to the SIEM database using the following command:

```
cat <plugin_name>.sql | ossim-db
```

Log Collection and Normalization in USM Appliance

The USM Appliance plugins process data collected from different data sources, parse and normalize the data, and save that data as standard format events in the SIEM database. Users can then view and analyze these events in the USM Appliance web UI.

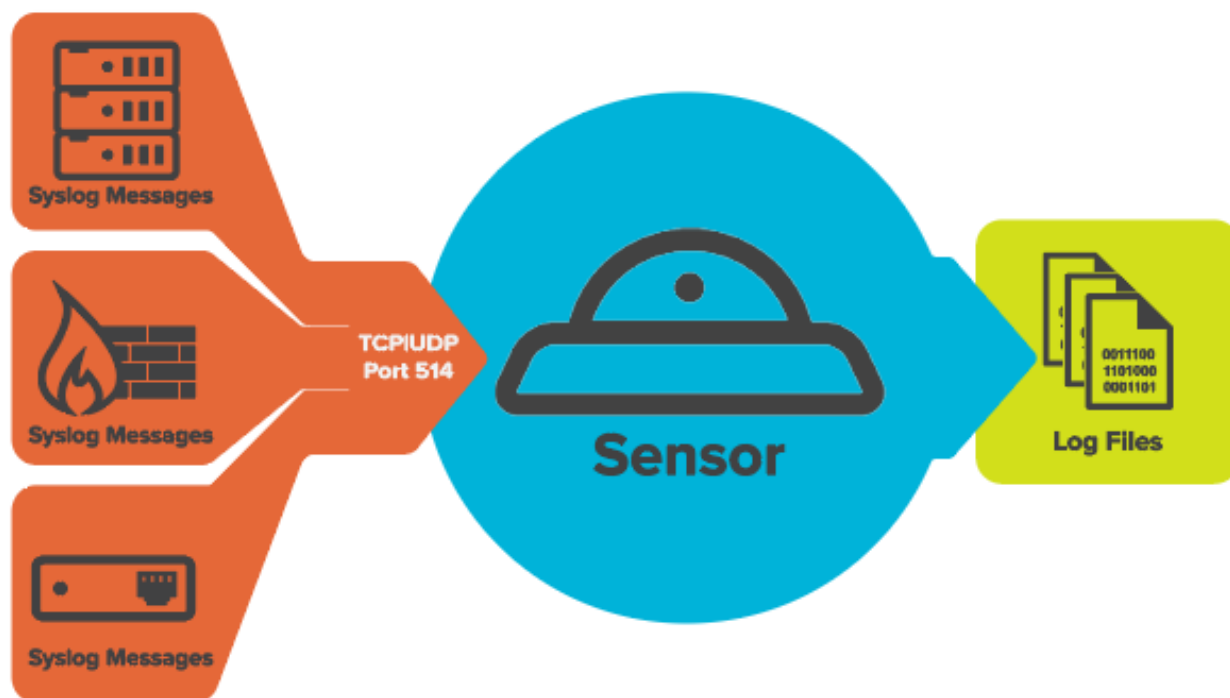
Plugins define

- how to collect information from an application or device
- how to normalize the collected information before sending data, in the form of standard format events, to the USM Appliance Server

A plugin is a software component that provides logic specific to extracting data collected from external applications and devices. Plugins are enabled in USM Appliance Sensors, which receive data from remote hosts using the following sources or protocols

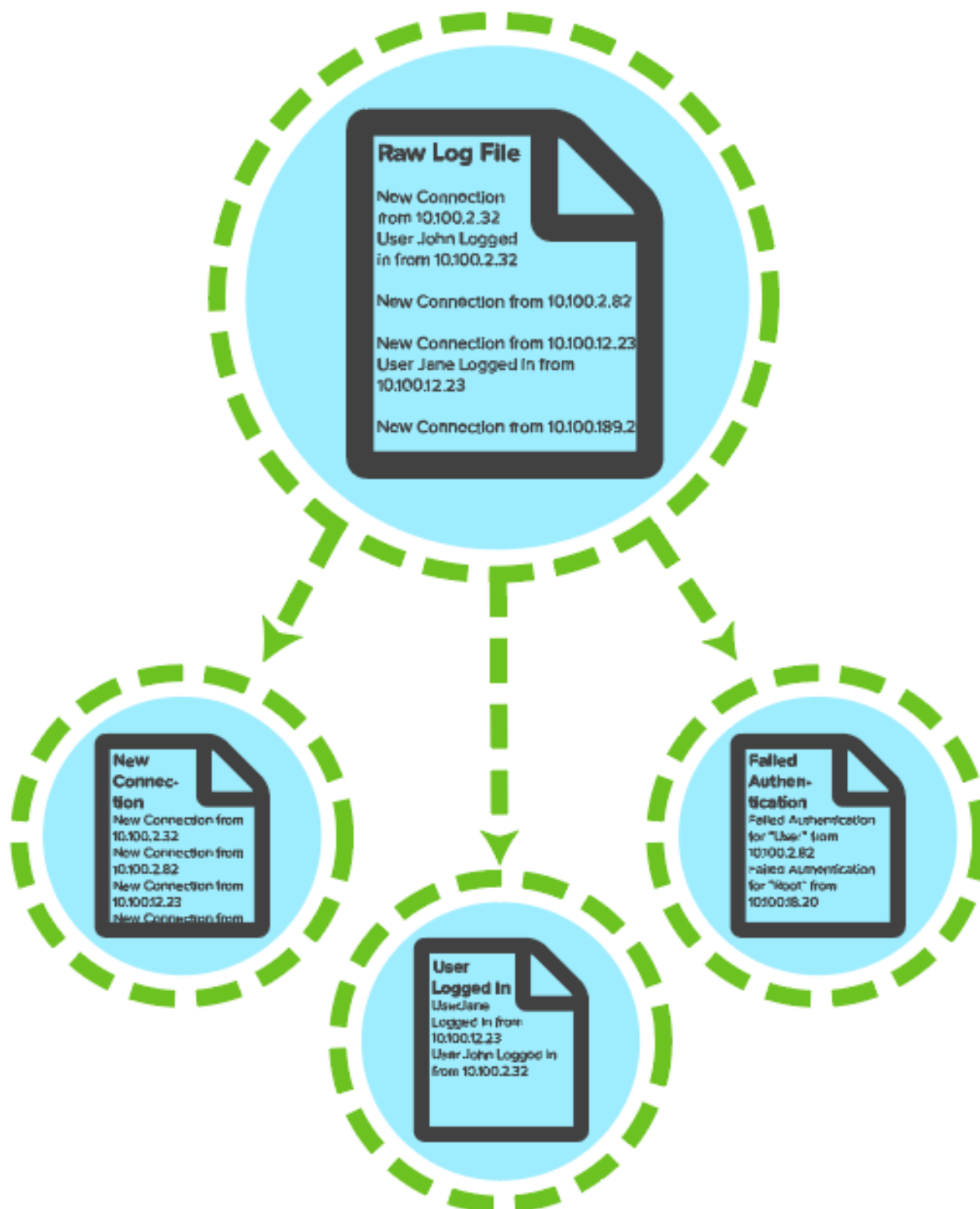
- Syslog
- Windows Management Instrumentation (WMI)
- Security Device Event Exchange (SDEE)
- Database
- Other protocols

Any system that processes logs requires a parser to read them, and to extract and convert their data into standard event fields. The following illustration shows the way in which a USM Appliance Sensor collects syslog messages from different devices, where enabled plugins can then process and normalize the event data contained in specific log files.



USM Appliance log collection diagram

During data normalization, a plugin evaluates information from each line of a log file and translates it to an event that identifies the event's type and subtype within the USM Appliance taxonomy. (See USM Appliance Event Taxonomy.) Normalization also converts portions of each log line into common data fields such as user, date and time, and source or destination IP address.



Log normalization process

Normalizing information into standard event data fields lets USM Appliance display information uniformly and also correlate events from various individual systems to generate alarms.


Plugin Types

The plugins included in USM Appliance are called detector plugins. They receive and extract events from logs, which include

- Text logs created by the `rsyslog` collection system.

USM Appliance uses `rsyslog` as its default syslog implementation. The configuration files of all external devices reside in `/etc/rsyslog.d`.

- Logs retrieved using other mechanisms such as SDEE (Security Device Event Exchange) or WMI (Windows Management Instrumentation).

 **Note:** For a current list of all AlienVault provided plugins, see the [data sheet](#).

The Source field of each plugin file indicates the type of detector plugin.

```
[config]
type=detector
enable=true
source=log
```

There are four types of detector plugins in USM Appliance, which are summarized in the following table.

Detector plugin types

Plugin Source	Description	Examples
Database	Monitors the content of external databases. Database plugins extract data from an external database and turn them into USM Appliance events. Supported databases are MySQL and Microsoft SQL Server. The database plugin configuration file provides information on how USM Appliance should connect to and query the database. See Configure Database Plugins for an example of database plugin configuration file and to obtain more information on configuring database plugins.	mcafee-epo
Log	Monitors a log file, usually receiving data through <code>syslog</code> . Log plugins extract events from log files by matching each line in a log file using a regular expression. The plugin then normalizes the information in the text to create events containing event field data from the text. See Configure Log Plugins for an example of log plugin configuration file and to obtain more information on configuring log plugins.	cisco-asa
SDEE	Monitors Cisco devices, using SDEE protocol. Cisco Systems IPS Sensor 5.0 uses the Security Device Event Exchange (SDEE) protocol to specify the format of messages used to communicate events generated by certain Cisco security devices. See Configure SDEE Plugins for an example of SDEE plugin configuration file and to obtain more information on configuring SDEE plugins.	cisco-ips
WMI	Remotely connects to Microsoft Windows events and data without an agent. Windows Management Instrumentation (WMI) plugins collect Microsoft Windows events and data remotely. These plugins collect the information, without an agent, using the Windows Management Instrumentation Command Line (WMIC). See Configure WMI Plugins for an example of WMI plugin configuration file and to obtain more information on configuring WMI plugins.	wmi-application-logger

Most detector plugins work automatically, without additional configuration, after you enable them. (See [Enable Plugins](#).)

IDM Plugins

IDM Plugins are a special type of detector plugin that collect additional information about devices and applications. This information is used to enhance the metadata of individual events when USM Appliance processes event data collected from other plugins. The IDM plugins in USM Appliance include

- arpalert-idm
- cisco-acs-idm
- linuxdhcp-idm
- nmap-hosts
- ossec-idm-single-line
- prads
- snare-idm



Note: The prads plugin, which identifies and collects information on network services running on hosts, is automatically enabled at startup, by default. Thus, no additional setup or configuration is required before you can start taking advantage of IDM information. Although not required, you can enable additional IDM plugins to gather information from different sources. For more information, see [Enable Plugins](#).

Scheduled inventory tasks such as asset discovery scans, WMI scans, and availability monitoring can also collect IDM information. Information collected by the IDM plugins and other scheduled processes is stored in an internal database, which also maintains historical data retrieved for the same hosts.

USM Appliance queries this data to enrich the metadata for events that are processed from other device and application-specific plugins. In addition, if values have changed in the historical data maintained for IDM data sources, the USM Appliance will generate an anomaly event that shows the change between the new and previous values. For more information on viewing anomaly events containing IDM information, see [Reviewing Security Events](#).

IDM information collected by host, based on their IP address, includes

- UUID, IP address, and domain of the host
- ID of the IDM source that generated the event (such as `nmap`, `ocs`, `nagios`)
- Hostname associated with the IP address
- MAC address
- Operating system
- CPU description and frequency
- RAM (in megabytes) on the host
- Host graphics cards
- List of users that have logged on or off

- List of active services
- List of software and hardware installed
- State of device or asset (on or off, up or down)

Plugin Updates

AlienVault USM Appliance notifies users when there is an update to the existing plugins, accessible from the USM Appliance Message Center.

These updates typically occur every two months. Starting with release version 5.4, plugin updates can also be scheduled and you can configure threat intelligence and plugin updates to run automatically. See [Update USM Appliance Online](#).



Note: The USM Appliance Sensor and USM Appliance Server must be updated independently.

Verify If There Is a New Plugin Update

To check if there is a plugin update, open the USM Appliance Message Center by clicking the envelope icon (✉).

If you see a message similar to "Plugins Feed Update - <YYYY-MM-DD>," it means that you have a plugin feed update. The Plugins Feed Update message displays the release notes, as shown.

ALIEN VAULT

WELCOME NBAENA | STABLE 172.16.100.1 | 30 SETTINGS SUPPORT LOGOUT

DASHBOARDS

ANALYSIS

ENVIRONMENT

REPORTS

CONFIGURATION

MESSAGE CENTER

Search

Unread (30)

All Messages (31)

Message Type

☐ Update (5)
 ☐ Deployment (1)
 ☐ Information (2)
 ☐ AlienVault (22)

Priority

☐ Info (30)
 ☐ Warning (0)
 ☐ Error (0)

DATE	SUBJECT	PRIORITY	TYPE	ACTIONS
2015-10-06 06:59:03	Configured DNS is external (172.16.100.1)	info	Deployment	
2015-10-05 20:00:00	New Update: AlienVault 5.2 has been released	info	Update	
2015-10-01 20:00:00	Upcoming USM and OSSIM updates	info	AlienVault	
2015-09-30 20:00:00	Plugins Feed Update - 2015-10-01	info	AlienVault	
2015-09-30 20:00:00	AlienVault Customer Satisfaction Survey - Your Input Requested, Please	info	AlienVault	
2015-09-14 20:00:00	Plugins Feed Update - 2015-09-15	info	AlienVault	

Plugins Feed Update - 2015-10-01

2015-09-30 20:00:00

Release Notes

Warning: This plugin feed release needs AlienVault 5.1 or greater.

New plugins available

- Linuxdhcp-idm: IDM plugin for linux DHCP

Issues fixed

- Yara: fixed naming
- Pam-unix: improved log matching
- F5: improved log matching
- VMware-vCenter: added v5.x support and improved log matching
- Fixed empty taxonomy for several plugins

Update Plugins

To install the latest plugin updates

1. Go to **Configuration > Deployment > Components > AlienVault Center**.
2. Review information about what the plugin package contains by clicking the Arrow icon (↓)


DEPLOYMENT ?

COMPONENTS **PLUGIN BUILDER** LOCATIONS

ALIENVAULT CENTER | SENSORS | SERVERS

ALIENVAULT CENTER

ALIENVAULT COMPONENTS INFORMATION Search:

NAME	STATUS	RAM USAGE	SWAP USAGE	CPU USAGE	NEW UPDATES
alienvault [192.168.73.154] Server Sensor Web Interface Database	UP	75.80 %	99.70 %	9.10 %	Patch 5.5.1 

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

3. Click **Update Feed Only**.

ALIENVAULT PACKAGE INFORMATION

PACKAGE	LATEST VERSION	SIZE
alienvault-agent-generator	5.5.1-3	468 kB
alienvault-apache2	5.5.1-3	4488 B
alienvault-api	5.5.1-3	72.4 kB
alienvault-api-core	5.5.1-3	9901 kB
alienvault-clean-sessions	5.5.1-3	3276 B
alienvault-cpe	1002-10	1095 kB
alienvault-crosscorrelation-pro	9.0.1-4038	64.0 kB
alienvault-crypto	5.5.1-3	5534 B
alienvault-depmo	5.5.1-3	3546 B
alienvault-directives-pro	10:9.0.1-4038	536 kB

SHOWING 1 TO 10 OF 220 ENTRIES FIRST PREVIOUS 1 2 3 4 5 NEXT LAST

CHECK FOR NEW UPDATES
UPDATE FEED ONLY
UPDATE ALL



Note: If you choose the **Update All** option, instead of **Update Feed Only**, USM Appliance applies a full system upgrade, which will include any plugin updates that are available.

Enable Plugins

AlienVault provides more than one way to enable plugins in USM Appliance. First, you can enable plugins on specific discovered assets, or you can enable plugins globally on USM Appliance Sensors. In addition, based on the specific plugin, you can enable plugins using different tools, including the USM Appliance web UI, the Getting Started Wizard, or the AlienVault console.

The following topics provide more information about the two choices available for enabling plugins.

- [Enable Plugins on Assets](#)
- [Enable Plugins from the Sensor Configuration](#)



Important: Be careful not to enable the same plugin twice, because this will generate duplicate events.

Below is a list of plugins that can only be enabled at the sensor level.

Plugin Name	Description
av-useractivity	A MySQL database plugin.
drupal-wiki	A MySQL database plugin.
eljefe	A MySQL database plugin.
linuxdhcp-idm	An IDM plugin for Linux DHCP server.
monit	Plugin for the <code>monit</code> service used in USM Appliance.
moodle	A MySQL database plugin.
ossec-idm-single-line	An IDM plugin for AlienVault HIDS.
ossec-single-line	Also known as the AlienVault HIDS plugin. Enabled by default.
post_correlation	A MySQL database plugin.
prads	An IDM plugin for passive asset discovery. Enabled by default.
ssh-remote	A plugin for OpenSSH.
suricata	Also known as the AlienVault NIDS plugin. Enabled by default.

For those plugins that allow it, enabling plugins on specific assets is generally recommended over enabling plugins on the USM Appliance Sensor. Plugins enabled at the asset level are automatically configured, whereas plugins enabled at the sensor level must often be configured first. For log-based plugins, this means setting up `rsyslog` collection and processing, and log rotation. (See [Configure the USM Appliance Sensor to Receive Logs Through Syslog](#).)

Convenience and performance may also be factors in choosing whether to enable plugins on individual assets, or to enable them on the USM Appliance Sensor. Enabling plugins on individual assets can help distribute the load of handling heavy traffic by running copies of the plugin on multiple processors or cores, rather than on a single one. However, if you want to use the same plugin with a large number of assets, and volume of traffic is not an issue, you may find it easier to enable and configure the plugin on the sensor.



Note: In addition to enabling the plugin, you must also configured the application or device that the plugin is intended for to forward its log to USM Appliance. For your convenience, AlienVault has composed a list of most commonly used devices and how to configure log forwarding on them. See [Configure Log Forwarding on Commonly Used Data Sources](#).


Enable Plugins on Assets

After you run a scan of your network to discover assets, the discovered assets are saved in the USM Appliance database. (For information on asset discovery, see [Adding Assets by Scanning for New Assets](#).) You can then select and enable plugins on the discovered assets. You can enable up to 10 plugins per asset.

Enabling Plugins from Asset Details in the Web UI

You can enable all plugins on an asset, *except* for the [sensor-only ones](#), from the USM Appliance web UI.

To enable a plugin from the Asset Details display

1. Go to **Environment > Assets & Groups > Assets**.
2. Select the asset for which you want to enable plugins.
3. Click the magnifying glass icon (.
4. Click the **Plugins** tab.
5. Click **Edit Plugins**.

EDIT PLUGINS

VENDOR

MODEL

VERSION

Cisco

ASA Adaptive Security Appliance

-

ADD PLUGIN

CANCEL

SAVE

6. Select a vendor, a model, and a version of the plugin you want to enable.
7. Click **Add Plugin**.
8. If you want to add another plugin, select another plugin in the same way as before and **click Add Plugin**; otherwise, click **Save**.

Enabled plugins now appear in the plugin display for the current asset:

VULNERABILITIES	ALARMS	EVENTS	SOFTWARE	SERVICES	PLUGINS	PROPERTIES	NETFLOW	GROUPS
EDIT PLUGINS								
VENDOR	MODEL	VERSION	SENSOR	RECEIVING DATA				
Cisco	ASA Adaptive Security Appliance	-	stable [172.16.100.1]	No				
<div>ADD NOTE</div>								

The Receiving Data value turns green when the Source, Destination, or Device IP field of an event matches the IP address of the asset.

9. Repeat the procedure for each discovered asset.

Note: Incoming syslog messages for each asset are saved on the USM Appliance Sensor in individual `/var/log/alienvault/devices/<asset_IP_address>` folders, one folder per asset IP address.

Enabling Plugins on Assets Using the Getting Started Wizard

You can enable all plugins, *except* for the [sensor-only ones](#), from the Getting Started Wizard, as long as you have USM Appliance All-in-One.



Note: The Getting Started Wizard is only available for USM Appliance All-in-One.

The Getting Started Wizard takes you through the initial setup tasks needed to configure USM Appliance after deployment.

After the wizard guides you through the network scan, you will see a list of discovered assets on the Log Management page. This page lets you enable up to 10 plugins for each of these discovered assets and up to 100 plugins per USM Appliance Sensor.

To enable plugins for each asset

1. Select the correct **Vendor**, **Model**, and **Version number** corresponding to the data that you want to collect from that asset.

All three fields are required. The Version field defaults to '-' if no other selection is available. The **Add Plugin** button is enabled.

2. If you want to enable another plugin for the same asset, click **Add Plugin**.

Another row is added for you to select the Vendor, Model, and Version number for a different plugin.

3. Repeat step 1 and 2 for each plugin you want to enable. You can enable up to 10 plugins per asset.

Set up Log Management

During the asset discovery scan we found 2 network devices on your network. Confirm the vendor, model, and version of the device shown. Click the "Enable" button to enable the data source plugin for each device.

ASSET	VENDOR	MODEL	VERSION	
Host-192-168-73-2 (192.168.73.2)	Cisco	ASA Adaptive Se...	-	
	Citrix	NetScaler	-	
	ADD PLUGIN			
Host-192-168-73-155 (192.168.73.155)	Select Vendor	Select Model	Select Version	
	ADD PLUGIN			

ENABLE

4. Repeat step 1-3 for each asset.

- To enable the selected plugins, click **Enable**.

The Log Management Confirmation page, shown in the following illustration, displays the plugins that you enabled. The Receiving Data value turns green when the Source, Destination, or Device IP field of an event matches the IP address of the asset. Gray means that no data is being received.

Set up Log Management

Plugin(s) successfully configured. Configure each asset to send logs by clicking on the instructions provided. Once the asset is configured AlienVault should detect the incoming data. When AlienVault receives data for a asset the "Receiving Data" light will turn green. Click "Finish" when you have received data from at least one asset.

ASSET	TYPE	PLUGIN ENABLED	RECEIVING DATA	INSTRUCTIONS
Host-192-168-73-2 (192.168.73.2)	Cisco ASA Adaptive Security Appliance	●	●	Instruction to forward logs
Host-192-168-73-2 (192.168.73.2)	Citrix NetScaler	●	●	Instruction to forward logs

- To learn how to configure your assets to send data to USM Appliance, click **Instructions to forward logs**.

After you have enabled plugins for your assets, click **Next** at the bottom-right corner to proceed.

Enable Plugins from the Sensor Configuration

You can enable up to 100 plugins on a USM Appliance Sensor from the USM Appliance web UI or from the AlienVault Console.

- [Enabling Plugins on the Sensor in the Web UI](#)
- [Enabling Plugins from the AlienVault Console](#)

Enabling Plugins on the Sensor in the Web UI

The USM Appliance web UI provides the fastest way to enable plugins on the sensor, particularly, if you have USM Appliance All-in-One.

To enable a plugin on the sensor configuration page in the USM Appliance web UI

- In the USM Appliance web UI, go to **Configuration > Deployment > Components > AlienVault Center**.
- Click one of the USM Appliance Sensors.
- Click **Sensor Configuration > Collection**.

SENSOR CONFIGURATION

OUTPUT DETECTION COLLECTION

Total number of plugins: 194

Plugins enabled		Plugins available	
5 items selected			
AlienVault_HIDS	—	AlienVault_HIDS-IDM	+
AlienVault_NIDS	—	W2003DNS	+
availability_monitoring	—	airlock	+
pam_unix	—	aix-audit	+
ssh	—	aladdin	+
		allot	+
		alteonos	+
		amun-honeypot	+

APPLY CHANGES

The left column of the Sensor Configuration page shows the enabled plugins. The right column shows the plugins available for enablement.

4. Move a plugin from one side to the other in either of these ways:
 - Drag a plugin from one column to the other.
 - Use the links [+] or [-] next to a specific item.
5. Click **Apply Changes**.
6. Configure `rsyslog` and `logrotate`. For instructions, see [Configure the USM Appliance Sensor to Receive Logs Through Syslog](#).

Enabling Plugins from the AlienVault Console

You can enable all plugins on the sensor from the AlienVault Console. However, you may find it's faster to enable plugins through the USM Appliance web UI, if you have USM Appliance All-in-One.

To enable plugins from the AlienVault Console

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

The AlienVault Setup menu displays.

2. Select **Configure Sensor**.
3. Select **Configure Data Source Plugins**.

4. Use the keyboard arrow keys to move to the plugin, select the plugin by pressing the spacebar, and then press Enter (<OK>).
5. Press <Back> until you are on the AlienVault Setup menu again. Select **Apply all Changes**.
6. Press <Yes> to confirm.

USM Appliance applies the changes and restarts all the services, which may take several minutes.

7. Configure `rsyslog` and `logrotate`. For instructions, see [Configure the USM Appliance Sensor to Receive Logs Through Syslog](#).



Note: If you want to confirm that the correct plugin has been enabled, jailbreak the system and open `/etc/ossim/agent/config.cfg`. The new plugin will appear inside the `[plugins]` section.

Verify that an Enabled Plugin Is Working Properly

It's good practice to test whether or not a plugin is working correctly, after you have enabled it in USM Appliance and configured the application or device to forward logs to USM Appliance.



Note: You can confirm the plugins enabled at the sensor level by viewing the `[plugin]` section of the `/etc/ossim/agent/config.cfg` file. Per-asset plugin configurations are stored in the `/etc/ossim/agent/config.yml` file.

To confirm an enabled plugin is working properly

1. In the USM Appliance web UI, go to **Analysis > Security Events (SIEM)**.
2. In **Data Sources**, select the plugin for which you expect to see events.

SECURITY EVENTS (SIEM)

SIEM REAL-TIME EXTERNAL DATABASES

Search Event Name GO

SHOW EVENTS

☒ Last Day
☐ Last Week
☐ Last Month
☐ Date Range

DATA SOURCES Ssh
 DATA SOURCE GROUPS
 SENSORS ☐ EXCLUDE
 ASSET GROUPS
 NETWORK GROUPS
 RISK
 OTX IP REPUTATION
 OTX PULSE
 Pulse name
☐ ONLY OTX PULSE ACTIVITY

userdata1 like Userdata1 field Device IP

CLEAR FILTERS

ADVANCED SEARCH

EVENTS GROUPED TIMELINE

SHOW TREND GRAPH Off

CHANGE VIEW ACTIONS

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS. 34,801 TOTAL EVENTS IN DATABASE.

EVENT NAME	DATE GMT-4:00	SENSOR	OTX	SOURCE	DESTINATION	RISK
SSHd: Connection closed	2016-07-18 17:56:54	staging	N/A	staging	staging:22	LOW
SSHd: Did not receive identification string	2016-07-18 17:56:48	staging	N/A	88.198.15.24	staging:22	LOW
SSHd: Did not receive identification string	2016-07-18 17:55:48	staging	N/A	88.198.15.24	staging:22	LOW
SSHd: Did not receive identification string	2016-07-18 17:55:47	staging	N/A	88.198.15.24	staging:22	LOW
SSHd: Did not receive identification string	2016-07-18 17:55:46	staging	N/A	88.198.15.24	staging:22	LOW

If you see events, the plugin is working properly.

If there are no events, you can troubleshoot by following the steps below.

To confirm receipt of syslog data from remote devices

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. Validate that you are receiving syslog packets from the source device.

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

Replace `<device_IP_Address>` with the IP address you are collecting syslog data from.

If no packets appear in the output, then USM Appliance is not receiving data from your device. Please make sure that you have configured your device or application to forward logs to the USM Appliance Sensor.

If the output shows the captured packets, it suggests that the issue is not the connection. Next, you can check if the syslog messages arrive in the correct log locations.

To confirm that syslog data appears in a log file

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. Check log files for new messages.

Messages from your device appear in different files depending on how the plugin is enabled.

- If the plugin is enabled on a per-asset basis, incoming syslog messages are saved in `/var/log/alienvault/devices/<asset_IP>`, one folder per asset IP address.

```
tail -f /var/log/alienvault/devices/<asset_IP>/<asset_IP>.log
```

- If the plugin is enabled at the sensor level, `rsyslog` is often configured to forward messages to a unique file, which is defined in the `location` parameter under the `[config]` section of the plugin file. After you have identified the file, type the following

```
tail -f /path/to/<data-Source-name>.log
```

- If syslog messages do not appear in either files mentioned above, you can check the default location for all syslog messages.

```
tail -f /var/log/syslog
```

If you do not find new messages in the corresponding log file, but you have confirmed that USM Appliance is receiving packets from your device through UDP port 514, verify that the `rsyslog` configuration directs the messages to the correct file. Restart `rsyslog` if needed.

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

If you see new messages in the log files, but there are no events, the error is in either the plugin or the agent configuration.

To verify that the plugin is generating events

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 **Troubleshooting Tools**.
4. Select **View AlienVault Components Logs**.
5. Select **View AlienVault Agent log**.

After confirmation, the content of `/var/log/alienvault/agent/agent.log` will be displayed in the console. You can press "q" to return to the menu.

6. Search for the plugin name in the log file.

For example, type `/ssh` and press Enter. If the plugin is running, you should see output similar to the following

```
WatchDog[24430] Checking process sshd for plugin ssh
WatchDog[24430] plugin (ssh) is running
WatchDog[24430] plugin (ssh) is enabled
```

7. In addition, you will see information about the plugin outputted every 10 seconds. For example

```
Aug 10 13:01:24 Alienvault-Agent[INFO]: ssh[4003] Total lines [12759]
TotalEvents:[643] EPS: [0.00] elapsed [10.01] seconds
Aug 10 13:01:34 Alienvault-Agent[INFO]: ssh[4003] Total lines [12759]
TotalEvents:[643] EPS: [0.00] elapsed [10.00] seconds
Aug 10 13:01:44 Alienvault-Agent[INFO]: ssh[4003] Total lines [12859]
TotalEvents:[683] EPS: [4.00] elapsed [10.00] seconds
```

where

- `Total lines [12759]` shows the number of lines (in the data source log file) that the plugin has processed after it is enabled.
- `TotalEvents: [643]` shows the number of events that the plugin has generated from those lines.
- `EPS: [0.00]` means Event Per Second and it is calculated every 10 seconds.

EPS 0.00 indicates that zero event has been generated in the last 10 seconds; EPS 4.00

indicates that 40 events (683 - 643) have been generated in the last 10 seconds.

- `elapsed [10.01] seconds` indicates that this information is gathered every 10 seconds.

`Total lines` and `TotalEvents` may not be the same because not every line can be turned into an event. If `TotalEvents` is 0, it means that the plugin has not generated any event. If `Total lines` is also 0, it means that the data source log file is empty, so the plugin has no data to process. But if `Total lines` is not 0, it means that the plugin does not turn those lines into events. You can look at the [plugin configuration file](#) to investigate further or contact [AT&T Cybersecurity Technical Support](#).

Configure Plugins

Most of the plugins in USM Appliance do not require additional configuration after they are enabled, especially if you [enable the plugin on an asset](#). But if you choose to [enable the plugin at the sensor level](#) and USM Appliance does not provide the required configuration files on the sensor, or if you are enabling a database plugin, an SDEE plugin, or a WMI plugin, you will need to perform some extra steps before the plugin can operate correctly.

This section describes the minimal configuration tasks for these plugin types. Most of the tasks require that you connect to the AlienVault Console through `SSH` and jailbreak the system to gain command line access. It is recommended that you are familiar with some basic Linux commands as well as a terminal-based text editor, such as `vim` or `nano`.

- [Configure Log Plugins](#)
- [Configure Database Plugins](#)
- [Configure SDEE Plugins](#)
- [Configure WMI Plugins](#)

Configure Log Plugins

Log plugins extract events from log files by matching each line in a log file using a regular expression. The plugin then normalizes the information to create events containing the data fields from the text.

Log Plugin Sample File

```
# Plugin ssh id:4003 version: 0.0.2
# Last modification: 2015-05-13 16:11
#
```

```

# Plugin Selection Info:
# OpenBSD:OpenSSH:-
#
# END-HEADER
# Accepted products:
# openbsd - openssh 5.4
# openbsd - openssh 5.5
# openbsd - openssh 5.6
# openbsd - openssh 5.7
# openbsd - openssh 5.8
# openbsd - openssh 5.8p2
# openbsd - openssh 5.9
# Description:

[DEFAULT]
plugin_id=4003
dst_ip=\_CFG(plugin-defaults,sensor)
dst_port=22

[config]
type=detector
enable=true
source=log
location=/var/log/auth.log
create_file=true
process=sshd
start=no
stop=no
startup=/etc/init.d/ssh start
shutdown=/etc/init.d/ssh stop

[translation]
none=1
opened=25
publickey=2
version=22
throughput=23
closed=26
password=1

[0000 - Failed password]
event_type=event
regex=(?P<date>\w{3}\s+\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<dst>\S+) sshd\[\\d+\]:
Failed password for\s(?P<info>invalid user\s)?(?P<user>\S+)\sfrom\s
(?P<src>\S+)\sport\s(?P<sport>\d{1,5})
date={normalize_date($date)}
plugin_sid=1
src_ip={resolv($src)}
dst_ip={resolv($dst)}
src_port={$sport}

```

```

username={$user}
userdata1={$info}
userdata2={$dst}
device={resolv($dst)}

[0001 - Invalid user]
event_type=event
regexp=(?P<date>\w{3}\s+\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<dst>\S+)\ssshd\[\d+\]:
Invalid user (?P<user>\S+) from\s+(?P<src>\S+)
date={normalize_date($date)}
plugin_sid=3
src_ip={resolv($src)}
dst_ip={resolv($dst)}
username={$user}
device={resolv($dst)}
.
.
.
<Additional rule matching Regex expressions added, as needed>

```

Understanding the Plugin File

Every plugin monitors a different log file for new syslog messages. If the plugin is enabled at the sensor level, this log file is defined in the `location` parameter under the `[config]` section. For example

```

[config]
...
location=/var/log/auth.log

```

Log plugins extract events from logs by matching each line in the log according to a regular expression. The plugin then normalizes the data fields from the text. For example, when a log message arrives, as shown

```
Feb 8 10:09:06 server1 sshd[24472]: Failed password for dgil from 192.168.6.69
port 33992 ssh2
```

The `SSH` plugin matches it with a regular expression (regex) in the rule of

```

regexp=(?P<date>\w{3}\s+\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<dst>\S+)\sshd\[ \d+\]:
Failed password for\s(?P<info>invalid user\s)?(?P<user>\S+)\sfrom\s
(?P<src>\S+)\sport\s(?P<sport>\d{1,5})

```

As soon as a rule matches a log line, matching stops, no matter how many remaining rules may match. The regular expression also extracts the relevant information from the matched log line. The regex fields, shown in boldface in the above example, identify the text to be mapped to the Security Event fields.

As a second step, the plugin normalizes that information for presentation within the USM Appliance Security Event view.

```
Date = Feb 8 10:09:06
src_ip =192.168.6.69
Username = dgil
```

The data source log format dictates the level of detail needed to generate events. The data source could require either just a few rules or one particular rule for each event.

The field `plugin_sid` identifies each individual event. This field is assigned either to every rule or it can be based on a field captured from a log line.

```
[0000 - Failed password]
event_type=event
regex=(?P<date>\w{3}\s+\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<dst>\S+) sshd\[\d+\]:
Failed password for\s(?P<info>invalid user\s)?(?P<user>\S+)\sfrom\s
(?P<src>\S+)\sport\s(?P<sport>\d{1,5})
date={normalize_date($date)}
plugin_sid=1
src_ip={resolve($src)}
dst_ip={resolve($dst)}
src_port={$sport}
username={$user}
userdata1={$info}
userdata2={$dst}
device={resolve($dst)}
```

Configure the USM Appliance Sensor to Receive Logs Through Syslog



Important: This task is only required if you enable the Log plugin through [Enable Plugins from the Sensor Configuration](#). AlienVault strongly recommends that you enable Log plugins through assets for ease of use and maintenance, unless you want to use the same plugin for a large number of devices.

For text logs received through the `rsyslog` service running on USM Appliance, you need to define the syslog routing rules in the `rsyslog` configuration file, located in `/etc/rsyslog.d/`. You also need to add a configuration file for `logrotate`, located in `/etc/logrotate.d/`, to rotate the logs.

To add rules for `rsyslog` and `logrotate`

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. Create a new configuration file to filter incoming logs. For example,

```
nano -w /etc/rsyslog.d/01_<dataSource_name>.conf
```

Where <dataSource_name> is the name of the plugin. The prefix of 01_ ensures that the file is processed before the default USM Appliance configurations.

4. Add the following line to the configuration file to identify the devices from which you should receive logs.

```
if ($fromhost-ip == '<IP_Address_1>') or ($fromhost-ip == '<IP_Address_2>')
then <path>/<dataSource_name>.log
& stop
```

Where

- <path>/<dataSource_name>.log matches the file listed in the `location` parameter of the plugin file
- <IP_Address_1> is the IP address of the first device and <IP_Address_2> is the IP address of the second device.
- If you want to receive logs from more devices in different subnets, add more 'or' clauses using the same syntax, (`$fromhost-ip == '<IP_Address>'`).
- If you want to filter for a subnet or a range of IP addresses, you can use the (`$fromhost-ip startswith '<partial_IP>'`) syntax. For example, (`$fromhost-ip startswith '192.0.1.'`).
- You can also use (`$fromhost == '<hostname>'`) if DNS resolution is enabled in your network.

5. Save the file by pressing **Ctrl+W** and exit the editor by pressing **Ctrl+X**.
6. Restart the Syslog Collector.

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

The USM Appliance Sensor should now process the incoming logs as soon as you enable the plugin.

7. Create a new `logrotate` configuration file.

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

8. Add the following lines of code to the file

```
<path>/<dataSource_name>.log
{
```

```
# save 4 days of logs
rotate 4
# rotate files daily
daily
missingok
notifempty
compress
delaycompress
sharedscripts
# run a script after log rotation
postrotate
invoke-rc.d rsyslog rotate > /dev/null
endscript
}
```

You do not need to keep the source log files on USM Appliance for more than a few days. Rotating these files regularly maintains enough free disk space on USM Appliance for standard operations.

Configure Database Plugins

Database plugins extract data from an external database and turn them into Events. USM Appliance supports MySQL and Microsoft SQL Server using the UTF-8 character set encoding.

The database plugin configuration file provides information on how USM Appliance should connect to and query the database.

Database Plugin Sample File

```
# Plugin mcafee-epo id:4008 version: 0.0.2
# Last modification: 2015-05-13 16:11
#
# Plugin Selection Info:
# McAfee:ePolicy Orchestrator:-
#
# END-HEADER
# Accepted products:
# mcafee - epo_mcafee_virtual_technician 1.0.9
# Description:
# McAfee EPO plugin
# MSSQL connection can be configured using a static port or
# a dynamic port (using instances)
# Static port config:
# source_ip=database_addr_or_hostname
# source_port=database_port (empty = default port 1433)
#
```

```

# Dynamic port config:
# source_ip=database_addr_or_hostname\database_instance (note: only one '\')
# no source_port
#
[DEFAULT]
plugin_id=4008

[config]
type=detector
enable=yes
custom_functions_file=/etc/ossim/agent/plugins/custom_functions/mcafee_epo_
custom_functions.cfg
source=database
source_type=mssql
source_ip=
source_port=1433
user=db_user
password=db_pass
db=db_epo
sleep=60
process=
start=no
stop=no

[start_query]
query="SELECT TOP 1 AutoID FROM EPOEvents ORDER BY AutoID DESC"
regexp=

[query]
query="SELECT AutoID, CONVERT(nvarchar(40), AutoGUID), ServerID, DetectedUTC,
SourceIPV4, TargetIPV4, TargetUserName, TargetFileName, ThreatCategory,
ThreatEventID, ThreatSeverity, ThreatName FROM EPOEvents where AutoID > $1
ORDER BY AutoID"
regexp=
ref=0
plugin_sid=${$9}
date={normalize_date($3)}
src_ip={:mcafeeIP($4)}
dst_ip={:mcafeeIP($5)}
filename=${$8}
username=${$6}
userdata1=GUID {$2}
userdata2=ServerID {$2}
userdata3=Severity {$10}
userdata4=${$9}
userdata5=${$11}
userdata6=${$1}

```

Anatomy of the Plugin Configuration File

See below for a description of various sections in the database plugin configuration file above.

The Config Section

In the database plugin configuration file example, the section that starts with `[config]` tells USM Appliance how to connect to the database. This consists of the following parameters.

```
[config]
type=detector
source=database
source_type=
source_ip=
source_port=
user=
password=
db=
sleep=
```

Description of database connection parameters

Parameter	Description
<code>source_type</code>	Database type that USM Appliance supports, which is mssql or mysql.
<code>source_ip</code>	Fully qualified domain name, hostname, or IP address.
<code>source_port</code>	Port number of the external database.
<code>user</code>	Name of the user with access to the database.
<code>password</code>	Password for user with access to the database.
<code>db</code>	Machine name of the external database.
<code>sleep</code>	Duration, in seconds, between plugin queries to the database.

The Start_Query Section

To find the point where the database plugin should begin capturing data, USM Appliance uses a query called *start_query*. This query obtains the last row in a table identified by a sequence number. The following code example initiates a query to select the largest AutoID number from the EPOEvents table.

```
[start_query]
query="SELECT TOP 1 AutoID FROM EPOEvents ORDER BY AutoID DESC"
```


The Query Section

USM Appliance queries the database as soon as a database plugin is loaded and, thereafter, every few seconds.

The duration between queries depends on the value of `sleep` in each plugin's configuration file. Default values range from 2 to 60 seconds and are configurable. For information about customizing existing or developing new plugins, see [Customize and Develop New Plugins](#) and its related topics.

This query starts with `[query]` and also references the `[start_query]` code line, shown in **bold** below.

```
[query]
query="SELECT AutoID, CONVERT(nvarchar(40), AutoGUID), ServerID, DetectedUTC,
SourceIPV4, TargetIPV4, TargetUserName, TargetFileName, ThreatCategory,
ThreatEventID, ThreatSeverity, ThreatName FROM EPOEvents where AutoID > $1
ORDER BY AutoID"
regexp=
```



Important: You must leave the `regexp` field empty (shown below the query), because database plugins use it in operation.

Fields containing \$ correspond to fields in the database query. For example

\$0	First element in the query (AutoID)
\$1	Second element in the query (AutoGUID)
\$2	Third element in the query (ServerID)
...

And you can map them to any of the event fields, like this

```
username={$6}
userdata1=GUID {$2}
userdata2=ServerID {$2}
userdata3=Severity {$10}
userdata4={$9}
userdata5={$11}
userdata6={$1}
```

Modify the Plugin Configuration File

Before modifying the plugin configuration file, you must first obtain the IP address, port number, and an authenticated user account of your database.



Warning: For Microsoft SQL Servers, you must use SQL Server Authentication. You will receive a "Connection refused" error if you use Windows Authentication instead.

This task enables communication with the external database from which the plugin receives data. You will need command line access to USM Appliance to complete this task.

To configure communication with an external database

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. Create the file `/etc/ossim/agent/plugins/<database-plugin>.cfg.local`.

For example, to configure the `mcafee-epo` plugin, you need to create the `mcafee-epo.cfg.local` file.

4. In the `.local` file, add the fields shown below and replace the angle bracket part (including the brackets) with your database settings.

```
[config]
source_ip=<database_IP>
source_port=<database_port>
user=<username>
password=<user_password>
db=<database_name>
sleep=<number_of_seconds_between_sending_queries>
```

5. Save the file.
6. Restart all services for changes to apply:

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



Important: If connecting to multiple databases, you must repeat this task for every external database you want to receive data from. In other words, you must create a different `<database-plugin>.cfg.local` file for each database you want to connect to.

If you do not see any events in **Analysis > Security Events (SIEM)** after you have modified the plugin configuration file and enabled the plugin, you can troubleshoot the database connection using `tcpdump` or `ngrep`. The following example examines the traffic to a MSSQL database.

```
ngrep -d eth0 host 10.10.10.10
```

where 10.10.10.10 is the IP address of the database server. If the database connection is established, you will see output similar to the following. You can confirm the user name, password, and database name (high-lighted in bold) from the output.

```
interface: eth0 (10.10.10.10/255.255.255.224)
filter: (ip or ip6) and ( host 10.10.10.10 )
.....
#####
T 10.10.10.20:54983 -> 10.10.10.10:1433 [AP]
.....10.10.10.10.....siem..... PASSWORD
.....37876.....pymssql.....10.10.10.10.....
..... PASSWORD.....DB-Library.....us_english.....
.....L.....ANSI_X3.4-1968.....512.....
#
T 10.10.10.10:1433 -> 10.10.10.20:54983 [AP]
.....g.....ePO4_HOSTNAME17.master.B.E.....-.Changed database context to
'ePO4_HOSTNAME17'..HOSTNAME15.....iso_1... ..Microsoft SQL
Server.._.....512.512.....
```

If the database connection cannot be established, you will receive an error instead.

Configure SDEE Plugins

Cisco Systems IPS Sensor 5.0 uses the Security Device Event Exchange (SDEE) protocol to specify the format of messages used to collect events generated by certain Cisco security devices. AlienVault supports this type of log collection and USM Appliance captures events specifically from

- Cisco Network Prevention Systems (IPS)
- Cisco Network Detection Systems (IDS)
- Cisco Switch IDS
- Cisco IOS routers with the Inline Intrusion Prevention System (IPS) functions
- Cisco IDS modules for routers
- Cisco PIX Firewalls
- Cisco Catalyst 6500 Series firewall service modules (FWSMs)
- Management Center for Cisco Security Agents
- CiscoWorks Monitoring Center for Security

SDEE Plugin Sample File

```
# Plugin cisco-ips id:1597 version: 0.0.2
# Last modification: 2015-05-13 16:11
#
```

```

# Plugin Selection Info:
# Cisco:IPS Intrusion Prevention System:-
#
# END-HEADER
# Accepted products:
# cisco - intrusion_prevention_system 6.0
# cisco - intrusion_prevention_system 6.0.2.0
# cisco - intrusion_prevention_system 7.0
# cisco - intrusion_prevention_system 7.0%281%29e3
# cisco - intrusion_prevention_system 7.0%282%29e3
# cisco - intrusion_prevention_system 7.0%282%29e4
# cisco - intrusion_prevention_system 7.0%283%29e4
# cisco - intrusion_prevention_system 7.0%284%29e4
# cisco - intrusion_prevention_system 7.0%285a%29e4
# cisco - intrusion_prevention_system 7.0%286%29e4
# cisco - intrusion_prevention_system 7.0%287%29e4
# cisco - intrusion_prevention_system 7.0%288%29e4
# cisco - intrusion_prevention_system 7.0%289%29e4
# cisco - intrusion_prevention_system 7.1
# Description:
# http://www.cisco.com/c/en/us/products/security/intrusion-prevention-system-
ips/index.html
#
#
[DEFAULT]
plugin_id=1597
[config]
type=detector
enable=yes
source=sdee
source_ip=
user=
password=
sleep=5
process=
start=no
stop=no

```

Working with the SDEE Devices

Each time a new session begins with a SDEE device, USM Appliance provides a subscription ID. (The latest Subscription ID can be found under `/etc/ossim/agent/sdee_sid.data`.)

To see messages related to the subscription

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. Enter

```
grep subs /var/log/ossim/agent.log
```

Normally, when the session finishes, the AlienVault Agent service closes the session automatically. If it does not, you should do it manually.

To close the last session

- Enter

```
python /usr/share/ossim/scripts/closeSDEEsession.py <SubscriptionID>
```

If you still have problems, look for the SDEE-related messages in the agent log.

To find SDEE messages in the agent log

- Enter

```
grep SDEE /var/log/ossim/agent.log
```

Additional Configuration Required Before You Enable an SDEE Plugin

You must configure USM Appliance to accept events from SDEE-capable devices from your USM Appliance assets before you enable the plugin.

- [Configuring USM Appliance to Accept Events from an SDEE-Capable Device](#)
- [Configuring USM Appliance to Accept Events from Multiple SDEE-Capable Devices](#)
- [Applying New Cisco IPS Signatures](#)

Configuring USM Appliance to Accept Events from an SDEE-Capable Device

This procedure describes how to configure the AlienVault Agent service to accept events from an SDEE-capable device. You will need command line access to USM Appliance to complete this task.

To configure USM Appliance to collect events from an SDEE device

1. Create the file `/etc/ossim/agent/plugins/cisco-ips.cfg.local`.
2. In the `cisco-ips.cfg.local` file, add the following lines.

```
[config]

source_ip=<source_IP>
user=<your_user>
password=<your_password>
```

Where

- `source_ip` is the IP address of the SDEE device.
- `user` is an user account for the SDEE device.
- `password` is the password for the user account on the SDEE device.

3. Save the file.

Configuring USM Appliance to Accept Events from Multiple SDEE-Capable Devices

To configure the AlienVault Agent service to accept events from multiple SDEE-capable devices, you will need command line access to USM Appliance to complete this task.

To configure USM Appliance to collect events from multiple SDEE devices

1. Create the file `/etc/ossim/agent/cisco_sdee.csv`.
2. In the `.csv` file, specify the IP addresses for the different SDEE devices and their login credentials. You must enter one device per line.

```
1.2.3.4,user1,pass1
1.2.3.5,user2,pass2
1.2.3.6,user3,pass3
```



Important: You must not have any empty lines after the credentials.

3. Create the file `/etc/ossim/agent/plugins/cisco-ips.cfg.local`.
4. In the `cisco-ips.cfg.local` file add the following lines. The `#` means to comment out those three lines.

```
[config]

#source_ip=
#user=
#password=

credentials_file=/etc/ossim/agent/cisco_sdee.csv
```

5. Save the file.

You can now enable the SDEE plugin. See [Enable Plugins on Assets](#).

Applying New Cisco IPS Signatures

Occasionally you may download or receive new signatures for your Cisco IPS devices. If you want to use those signatures in USM Appliance, you will need to update the USM Appliance database manually. You will need command line access to USM Appliance to complete this task.

To populate the USM Appliance database with new signatures

1. Go to `/usr/share/ossim/scripts/` and execute the following script to generate the plugin sid information.

```
python createCiscoIPSSidmap.py <signature_file>.xml > sdee.sql
```

where `<signature_file>.xml` is the file you downloaded or received from Cisco.

This script generates the `sql` needed to update the USM Appliance database.

```
DELETE FROM plugin WHERE id = "1597";
DELETE FROM plugin_sid where plugin_id = "1597";
INSERT INTO plugin (id, type, name, description) VALUES (1597, 1, 'Cisco-IPS',
'Cisco Intrusion Prevention System');
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority,
reliability) VALUES (1597, 5986, NULL, NULL, 'Cisco-IPS: Microsoft GDI GIF
Parsing
Vulnerability', 3, 4);
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority,
reliability) VALUES (1597, 5984, NULL, NULL, 'Cisco-IPS: IE COM Object
Code
Execution', 3, 4);
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority,
reliability) VALUES (1597, 5985, NULL, NULL, 'Cisco-IPS: Quicktime RTSP
Content-
Type Excessive Length', 3, 4);
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority,
reliability) VALUES (1597, 19159, NULL, NULL, 'Cisco-IPS: Green Dam Youth
Escort
Software Update Check', 1, 4);
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority,
reliability) VALUES (1597, 19401, NULL, NULL, 'Cisco-IPS: Microsoft
Publisher File
```

```
Parsing Vulnerability', 3, 4);
```

2. Update the USM Appliance database with the `sql` output.

```
ossim-db < sdee.sql
```

3. Generate the cross-correlation information.

```
python ciscoIPSOSMap.py <signature_file>.xml > sdee-os.sql
```

This script generates the following `sql` to update the USM Appliance database with cross-correlation information.

```
replace into plugin_reference values (1597, 1109, 3001, 3);
replace into plugin_reference values (1597, 1109, 3001, 3);
replace into plugin_reference values (1597, 1109, 3001, 3);
replace into plugin_reference values (1597, 1109, 3001, 3);
replace into plugin_reference values (1597, 2156, 3001, 1);
replace into plugin_reference values (1597, 2157, 3001, 3);
replace into plugin_reference values (1597, 2157, 3001, 3);
replace into plugin_reference values (1597, 2157, 3001, 3);
...
```

4. Update the USM Appliance database with the `sql` output.

```
ossim-db < sdee-os.sql
```

5. Clear the cache by restarting USM Appliance.

Configure WMI Plugins

Windows Management Instrumentation (WMI) plugins collect Microsoft Windows events and data remotely. These plugins collect the information without an agent, using the Windows Management Instrumentation Command Line (WMIC).



Note: Currently, WMIC does not support samba4/NTLMv2. Nor does WMIC work on more recent Windows versions, like Windows Server 2012 or later, because these versions authenticate with NTLMv2 only by default.

To use a WMI plugin with a Windows host that uses NTLMv2, you must manually enable NTLMv1 authentication. For information about this, see the Microsoft Support web pages.

WMI Plugin Sample File

```
# Plugin wmi-application-logger id:1518 version: 0.0.2
# Last modification: 2015-05-13 16:11
#
# Plugin Selection Info:
```



```
# AlienVault:WMI Application Logger:-
#
# END-HEADER
# Accepted products:
# alienvault - plugin-wmi -
# Description:
#
[DEFAULT]
plugin_id=1518
[config]
type=detector
enable=yes
source=wmi
credentials_file=/etc/ossim/agent/wmi_credentials.csv
sleep=10
process=
start=no
stop=no
[start_cmd]
cmd=wmic -U OSS_WMI_USER%OSS_WMI_PASS //OSS_WMI_HOST "Select
LogFile,RecordNumber from Win32_NTLogEvent Where Logfile = 'Application'" |
head -n 3 | tail -n 1 | cut -f 2 -d \
regexp=
[cmd]
cmd = wmic -U OSS_WMI_USER%OSS_WMI_PASS //OSS_WMI_HOST "Select
ComputerName,EventCode,Logfile,Message,RecordNumber,SourceName,TimeWritten,Us
er from Win32_NTLogEvent Where Logfile = 'Application' and RecordNumber > OSS_
COUNTER" | cat
start_regexp=^([^\|]+)\|(\d+)\|([^\|]+)\|
regexp="^(?P<system_name>[^\|]+)\|(?P<plugin_sid>\d+)\|(?P<logfile>[^\|]+)\|
(?P<message>[^\|]+)\|(?P<recordnumber>[^\|]+)\|(?P<sourcename>[^\|]+)\|
(?P<timewritten>[^\|]+)\|(?P<username>.*)$"
src_ip={resolv($0)}
plugin_sid=${1}
userdata2=${2}
userdata3=${3}
userdata4=${4}
userdata5=${5}
userdata6=${6}
username=${7}
```

The following sections of a WMI plugin are essential.

```
[start_cmd]
[cmd]
```

You use `[start_cmd]` and `[cmd]` to return the last WMI Application event, and start reading from that event.

Additional Configuration Required Before You Enable an WMI Plugin

You need to perform the following additional configuration before you can use the WMI plugins.

1. [Enable Remote WMI Access in a Microsoft Windows Host](#)
2. [Create a WMI Credentials File](#)
3. [Configure a Path to the WMI Credentials File](#)

Enable Remote WMI Access in a Microsoft Windows Host

This configuration procedure is for users who must contact the WMI plugin remotely from a Windows host. The procedure is appropriate for production.



Note: This procedure is based on Microsoft Windows 7. Microsoft Windows 10 no longer shows the Run box in the Start menu. However, Windows 10 does allow you to personalize the Start menu to include it. For more information, refer to the Windows 10 documentation.

To enable remote WMI access on Windows

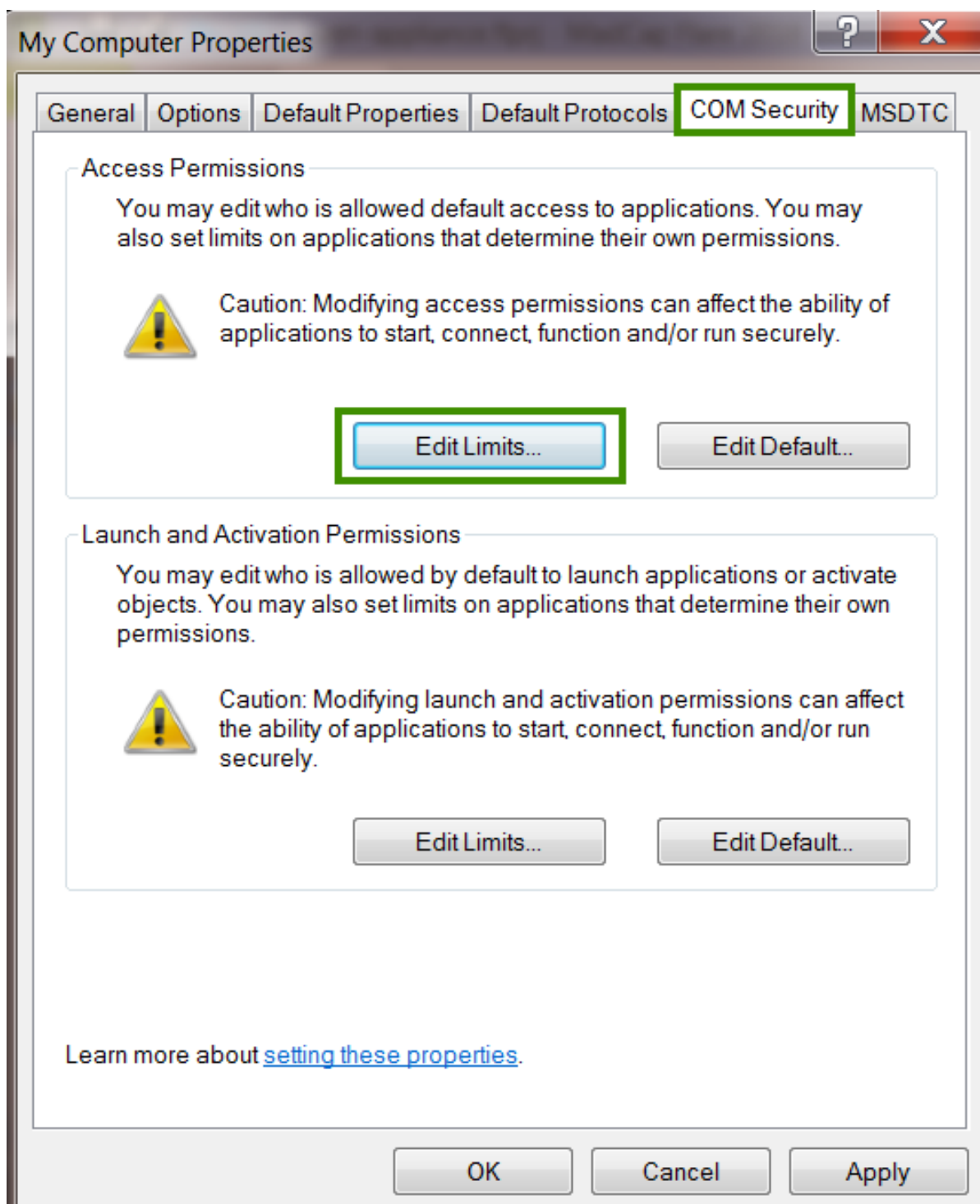
1. Create a new user in the Windows host (without any administrator privileges) who can connect remotely. In this example, we use “wmiuser” as the username and “wmi” as the password.



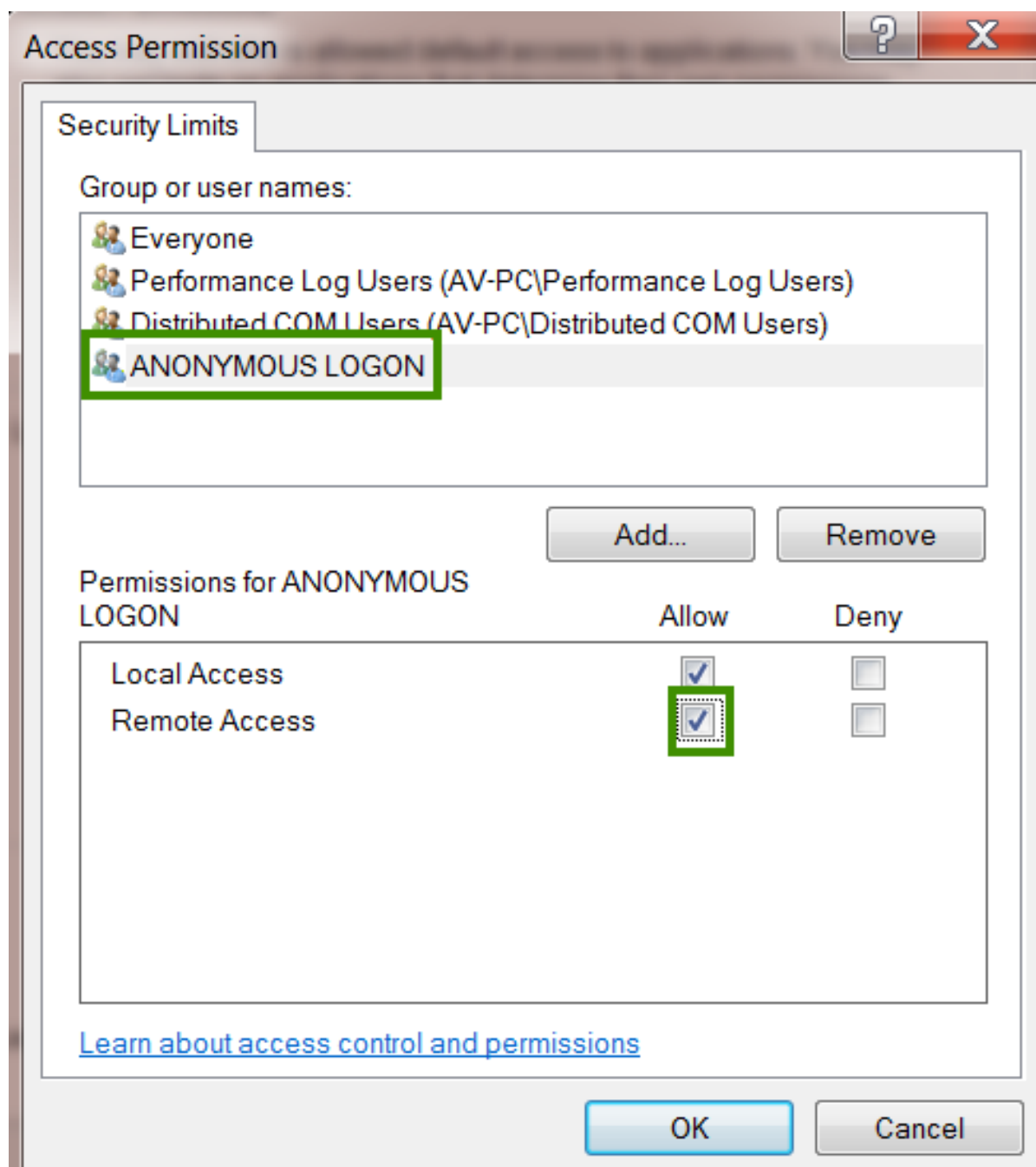
Important: This step is performed to make the connection more secure.

2. Enable remote access and activation permissions for the user account you just created.
 - a. In the Windows **Start** menu, type `Dcomcnfg` in the empty field and press Enter .
 - b. In the **Component Services** dialog box, right-click **My Computer** and select **Properties**.

- Click the **COM Security** tab, then **Edit Limits** under Access Permissions.



- Click **ANONYMOUS LOGON**, enable Allow **Remote Access**, and then click **OK**.



5. Click **Apply**.
6. On the **COM Security** tab, under Launch and Activation Permissions, select **Edit Limits**, then click **Add**.
7. In the empty field of the popup that appears, type the username for the new user account and click **OK**.

8. On the Launch and Activation Permissions dialog box, select **Remote Launch, Local Activation**, and **Remote Activation**. Click **OK**.
9. Click **Apply**, and then **OK**.

Create a WMI Credentials File

Follow this procedure to create a file with your Windows IP and credentials on USM Appliance. You will need command line access to USM Appliance to complete this task.

To configure USM Appliance to use a WMI plugin

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. Create a `wmi_credentials.csv` file.

```
vim /etc/ossim/agent/wmi_credentials.csv
```

4. Add IPs, users, and password with the following formats.

```
xxx.xxx.x.x,<domain_name>\\<wmiuser>,<password>
```

Example

```
233.200.7.0, mydomain_name\\mr_big,ugessed1t
```

If you do not use a domain, enter the following instead.

```
xxx.xxx.x.x, <username>,<password>
```

5. Save the file.

Configure a Path to the WMI Credentials File

In order for the WMI plugin to work correctly, you must update the plugin with the path to the `wmi_credentials.csv` file you just created. You will need command line access to USM Appliance to complete this task.

To specify the path to the WMI credentials file

1. Depending on which plugin you've enabled, locate the WMI configuration file or files in your USM Appliance instance. Potential file locations might be any of the following.

```
/etc/ossim/agent/plugins/wmi-application-logger.cfg
/etc/ossim/agent/plugins/wmi-monitor.cfg
/etc/ossim/agent/plugins/wmi-security-logger-srv2008.cfg
/etc/ossim/agent/plugins/wmi-security-logger.cfg
/etc/ossim/agent/plugins/wmi-system-logger.cfg
```

2. Create the file `<wmi-xxxx-plugin>.cfg.local` based on your choice and enter the path to your `wmi_credentials.csv` file in the `credentials_file` field.

Example

```
[config]
credentials_file=/etc/ossim/agent/wmi_credentials.csv
```

3. Save the file.

You can now enable the WMI plugin. See [Enable Plugins on Assets](#).

Customize and Develop New Plugins

AlienVault provides a large number of plugins as part of its default installation. In most environments this should cover the external applications and devices that you want to integrate. However, sometimes you may need a plugin with special properties or handling of events. Customizing a plugin refers to repurposing a particular type of existing plugin to better suit your needs. In most cases, customization does not change the plugin type.

Developing a plugin refers to creating a new plugin from scratch, typically to collect event from a particular device type for which no plugin currently exists. To create a new plugin, you can edit and configure all the plugin's configuration and regex settings by hand, or you can use the plugin builder wizard built into the USM Appliance web UI to simplify the process.

This section provides more information using each of these methods of customizing or creating new USM Appliance plugins.

Customize Existing Plugins Yourself

You may want to customize an existing plugin, for example, if you need to update configuration file settings, add or update rules, exclude events, or make regex expression changes.

Create the .local File

With any existing plugin file you want to make changes to, you must first create a new empty file with the same name and append the `.local` extension to the file:

```
<filename>.cfg.local
```

You can then add your changes to the plugin in the `.local` file. Only include the delta, or items you want to change from the original plugin file, along with the [section name](#) that it belongs to. For example, if you want the plugin to read from a different log file, you can specify the location for the log file like this:

```
[config]
```

```
location=/path/to/file
```

Changes in your `.local` file takes precedence over any settings defined in the original plugin file. The `.local` file will not be overwritten by system updates. You can change anything within a plugin file except the header or the `plugin ID`, `enable`, `type`, and `source` parameters.

If you want to modify an existing rule, either the `regex` parameter or any of the event field mappings, you must use the same rule ID. For example, if you want to modify the `[ssh - Failed password]` rule in the `SSH` plugin, you must include the `[ssh - Failed password]` section in your `.local` file and specify your changes underneath.



Important: AT&T Cybersecurity recommends that you keep any plugin file that you customized or developed until you can verify that AT&T Cybersecurity has included your requested revision in one of its biweekly updates.

Typical customization include but is not limited to

- [Exclude Event Type IDs Processed by Sensors](#)
- [Change Timezone for a Plugin](#)
- [Customize Plugin Date and Time Formats](#)
- [Define and Use Custom Functions](#)
- [Add a New Rule to a Plugin](#)

Exclude Event Type IDs Processed by Sensors

After enabling a plugin, the USM Appliance Sensor processes the plugin's log data and sends events it collects to the USM Appliance Server, where they are stored in the SIEM database. You can then view the events in the USM Appliance web UI by selecting the **Analysis > Security Events (SIEM)** option.

After using the plugin for a while, you may find a number of events that you don't find useful to display or track, and just create noise and take up space in the SIEM database. Rather than creating USM Appliance policies to filter out these events, which incurs some processing overhead, you can include the **exclude_sids** parameter in a `.local` copy of the plugin's configuration file to achieve the same result.

To exclude collection of specific event type IDs from a plugin

1. Connect to USM Appliance through SSH.
2. On the AlienVault Setup menu select **Jailbreak System**.
3. If the file does not already exist, create the file `/etc/ossim/agent/plugins/<plugin_name>.cfg.local`.
4. In the `<plugin_name>.cfg.local` file, add the `exclude_sids` parameter in the [CONFIG] section and specify one or more event type IDs (separated by commas) that you don't want the sensor to process. For example:

```
[CONFIG]
exclude_sids=200,302,404,403
```

5. Save the file and restart `ossim-agent`:

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

The SIDs you specify with the `exclude_sids` parameter are the Event Type IDs that USM Appliance assigns to each event that matches a specific rule in the plugin configuration file. The quickest way to locate the SID number of a specific event type is to go to the **Analytics > Security Events (SIEM)** page, and click on the row of a particular event you want to exclude. From the Event Detail display that is shown, you can locate the Event Type ID associated with the event. Use that value for the `exclude_sids` parameter in the plugin's configuration file.

EVENT DETAILS

AlienVault HIDS: Login session opened.

DATE	2017-06-22 16:47:45 GMT-4:00	CATEGORY	Authentication
ALIENVAULT SENSOR	devel [172.16.100.1]	SUB-CATEGORY	Login
DEVICE IP	172.16.100.1 [eth0]	DATA SOURCE NAME	AlienVault HIDS-authentication_success
EVENT TYPE ID	5501	DATA SOURCE ID	7009
UNIQUE EVENT ID#	578c11e7-9f6a-000c-2931-6aef12576d2a	PRODUCT TYPE	Authentication and DHCP
PROTOCOL	TCP	ADDITIONAL INFO	N/A

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

SOURCE	devel [172.16.100.1]	DESTINATION	devel [172.16.100.1]
Hostname: devel	Location: N/A	Hostname: devel	Location: N/A
MAC Address: N/A	Context: N/A	MAC Address: N/A	Context: N/A
Port: 0	Asset Groups: N/A	Port: 0	Asset Groups: N/A

Another way, in which you can view all the event type IDs associated with every plugin, is to go to the **Configuration > Threat Intelligence** page and select the **Data Source** tab. From there, each row of the display lists information about a plugin, and you can double-click on a specific row to view all the associated event type IDs for the selected plugin.

Change Timezone for a Plugin

If you have a plugin that processes logs from an asset located in a different timezone than your sensor, sometimes due to the source device using an incorrect timezone or a timezone that cannot be changed, you can modify the timezone in the plugin file instead. The following task shows how to do this using the `SSH` plugin as an example.

To change the timezone used by a plugin

1. Connect to USM Appliance through `SSH`.
2. On the AlienVault Setup menu select **Jailbreak System**.
3. Check the default timezone that `ossim-agent` uses.

```
~# grep tzone /etc/ossim/agent/config.cfg
tzone=Europe/Dublin
```

This should match the timezone of where your USM Appliance Sensor resides.

4. Create the file `/etc/ossim/agent/plugins/ssh.cfg.local`.
5. In `ssh.cfg.local`, add the following parameter:

```
[DEFAULT]
tzone=Australia/Melbourne
```

where

Australia/Melbourne represents the timezone of the asset you are collecting logs.



Note: USM Appliance validates timezones against [this list](#).

6. Save the file and then restart ossim-agent.

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

7. Check the agent log to make sure the new timezone has been applied:

```
~# grep -Al "Starting detector" /var/log/alienvault/agent/agent.log
2016-01-18 10:39:38,948 AlienVault-Agent [INFO]: Starting detector ssh
(4003)..Plugin tzone: Australia/Melbourne
2016-01-18 10:39:38,950 AlienVault-Agent [WARNING]: Using custom plugin
tzone data: Australia/Melbourne
```

Customize Plugin Date and Time Formats

Different devices often use different date and time formats in their logs. USM Appliance solves this issue by providing a built-in function, `normalize_date()`, which converts different date formats to ISO 8601, the format accepted by the USM Appliance Server. For a list of formats that the function recognizes, see [Supported Formats by the `normalize_date\(\)` Function](#).

If the date and time format is not supported by the `normalize_date()` function, for example, DD/MM/YYYY HH:MM:SS, you can create a custom function to handle the specific date and time format that you need.



Note: Existing date formats are defined in the `date_formats.json` file. Modifying this file is NOT recommended, since USM Appliance updates will overwrite any changes you make to the file.

The following example provides a template for a custom function named `normalize_date_not_american()`, in which you can define the patterns of date and time you want to format.

```
#
# Description:
#   This function should only be called when a date
#   is in this format:
#   12/08/2016 21:44:47
#   dd/mm/yyyy hh:mm:ss
#
# Usage:
```

```
#   date={:normalize_date_not_american( $date_log )}
#
Start Function normalize_date_not_american
from re import compile
from datetime import datetime
def normalize_date_not_american( self, string = "" ):
    pattern = compile( r'(?P<day>\d{1,2})/(?P<month>\d+)/
        (?P<year>\d{4})\s(?P<hour>\d+):(?P<minute>\d+)
        :(?P<second>\d+)' )
    result = pattern.search(string)
    groups = result.groupdict()
    date = datetime(year=int(groups['year']),
        month=int(groups['month']), day=int(groups['day']),
        hour=int(groups['hour']), minute=int(groups['minute']),
        second=int(groups['second'])).isoformat(' ')
    return date
End Function
```

After creating and saving the custom function, you can use it in the plugin configuration file. For more information on using custom functions in plugins, see [Define and Use Custom Functions](#).

Define and Use Custom Functions

In addition to the [built-in functions that USM Appliance supports](#), you may also create your own custom functions to convert extracted data to the format required by specific event field types.

To create a new custom function

1. In the Config section, specify the location of a new file containing one or more new function definitions.

```
[config]
custom_functions_file=/etc/ossim/agent/plugin/custom.cfg
```

2. Create a text file that matches the custom function's file name. In the new file, define the operation of each new custom function you want to create. Each new function must start with `Start Function <function_name>` and end with `End function`.

The following example shows the definition of two new functions , `log_hello` and `log_hello_data`.

```
Start Function log_hello
    def log_hello(self):
        return "Hello log!"
End Function
```

```

Start Function og_hello_data
  def log_hello_data(self,data):
    return "Hello log: %s" % data
End Function

```

In this example, the `log_hello()` function returns the string "Hello log!" and the value assigned to a normalized event field. The second function returns the "Hello log!" string concatenated with the extracted user name value.

3. Save and close the custom function file.



Note: Be careful if you add a custom function to a plugin or if you access a proprietary database. This can degrade performance if not well designed. Custom plugins might take up to five minutes to appear in the USM Appliance web UI after you add them.

4. To use the new custom functions, you can simply include as part of any event field assignment corresponding to extracted data returned for a specific rule or log event. For example

```

[ssh - Failed password]
# Feb 8 10:09:06 server1 sshd[24472]: Failed password for dgil from
192.168.6.69 port 33992 ssh2
event_type=event
regex="(\\w{3}\\s+\\d{1,2}\\s\\d\\d:\\d\\d:\\d\\d)\\s+(?P<sensor>\\S*)\\.ssh\\.Failed
password for
(?P<user>\\S+)\\s+from\\s+.*?(?P<src>\\IPV4)\\.port\\s+(?P<sport>\\d{1,5})"
plugin_sid=1
sensor={resolve($sensor)}
date={normalize_date($1)}
src_ip={$src}
dst_ip={resolve($sensor)}
src_port={$sport}
username={$user}
userdata1={:log_hello()}
userdata2={:log_hello_data($user)}

```



Important: You are not allowed to use a custom function in a built-in function, for example, `translate(:log_hello())`, as custom functions are the last functions to be executed in a rule.

Add a New Rule to a Plugin

The following task shows how to change an existing rule and add a new rule to a plugin, in this case, for Cisco ASA.

To change or add a rule to an existing plugin

1. Connect to USM Appliance through SSH.
2. On the AlienVault Setup menu select **Jailbreak System**.
3. Create the file `/etc/ossim/agent/plugins/cisco-asa.cfg.local`.
4. (As needed) Change any existing regex mappings or rules needed for the re-purposed plugin.

The following example shows the changed rule, in bold, as the value of the `regex` parameter. The commented section shows the mapping target of the `regex` parameter.

```
#Sep 17 06:25:31 5.5.5.5 : Sep 17 06:26:10 EDT: %ASA-ids-4-401004:
#Shunned packet: 1.1.1.1 ==> 1.1.1.2 on interface inside
[0001 - cisco-asa - Shunned packet]
regex="(P<date>\w{3}\s+\d{1,2}\s(\d{4}\s)?\d\d:\d\d:\d\d)\s*:?
((P<device>\S+)\s*:?)\s+[\w\:\s]*?(P<asa_short_msg>(asa|ASA)-[\w\:-]*-?
(\d+)-(P<sid>\d+)):\s+(P<userdata>[^:]+\s+(P<src_ip>\S+)\s+==>\s+
(P<dst_ip>\S+).*)"
```

5. (As needed) Add any new rule needed for the revised plugin, as shown in the following example. The commented section shows the mapping target of the `regex` parameter.

```
#Mar 28 12:03:04 testbox %ASA-7-609002: Teardown local-host inside:1.1.1.1
duration 0:02:12
[9000 - cisco-asa - Teardown local-host]
precheck="Teardown"
regex="(P<date>\w{3}\s+\d{1,2}\s(\d{4}\s)?\d\d:\d\d:\d\d)\s*:?
((P<device>\S+)\s*:?)\s+[\w\:\s]*?(P<asa_short_msg>(asa|ASA)-[\w\:-]*-?
(\d+)-(P<sid>\d+)):\s+(P<userdata>(?:Teardown\slocal-host\s)(P<iface>
[^:]*):(P<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}))\s\S+\s
(P<duration>\S+).*)"
event_type=event
date={normalize_date($date)}
device={resolve($device)}
plugin_sid={$sid}
src_ip={$src_ip}
userdata1={$asa_short_msg}
userdata2={$iface}
userdata3={$duration}
userdata4={$userdata}
```

6. Save the file and then restart ossim-agent:

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

7. Check regular expressions and also field assignments within the file `/var/log/cisco-`

```
asa.log.
```

We recommend that you use any of the utilities available on the Internet to test that the Python regular expressions you added match the logs.

After creating a new rule, you will also need to define a new event type ID to assign to events matching the new rule.

However, if you have many new event types to add, you should use the plugin `.sql` file instead, because it is much faster. The web UI is better when you have only one or two event types to add.



Note: If you do not perform this task, these events will not appear in the Security Events view in the USM Appliance web UI.

To add new event types

This procedure adds a custom event type to an existing or newly developed plugin, using the USM Appliance web UI.

1. Go to **Configuration > Threat Intelligence > Data Source**.
2. Double-click a data source to open it.
3. Click **Insert New Event Type**.

The Add New Event Type dialog box appears.

4. Fill in the fields, make value selections from the lists, and then click **Update**.

Add New Event Type fields

Field/List	Description
Name*	Event description. The text you introduce here refers to the event name, which appears in the Event Name column on the Security Events (SIEM) page.
Event type ID*	Refers to the <code>plugin_sid</code> . Note that you may not use a <code>plugin_sid</code> already in use. If you use the same ID twice, USM Appliance returns an error.
Category	Event type categories depend on the event type ID.

Add New Event Type fields (Continued)

Field/List	Description
Subcategory	Select a subcategory for the new event type. For example, an event type ID might have subcategories such as Attack, Brute Force, or Policy.
Reliability*	Values range from 0 to 10, with 10 being the greatest reliability.
Priority*	Values range from 0 to 5, with 5 being the highest priority.

Values with an asterisk (*) are required.

Default Functions Used in the USM Appliance Plugins

The USM Appliance Server must receive normalized events in a predefined format. USM Appliance provides a number of built-in functions you can use to convert the extracted data obtained from matching the regular expressions to the format expected in normalized USM Appliance event fields.

For example, time and date in USM Appliance is in the format of `YYYY-MM-DD HH:MM:SS` (for example, `2013-12-31 22:57:00`), but different data sources may use different formats for time and date. You can use the `normalize_date()` function, which simplifies the process of normalizing events, by converting different time formats into the format accepted by the server.

Another function often used is `resolve()`, which translates hostnames into IPv4 addresses by performing DNS queries.

```
date={normalize_date($date) }
dst_ip={resolve($dst_ip) }
src_ip={resolve($src_ip) }
```

The following table provides a list of the built-in USM Appliance functions.

USM Appliance default plugin functions

Function	Description
<code>geoip_getCity(addr)</code>	Returns the corresponding city name according to the built-in GeoIP database.
<code>geoip_getCountryCode(addr)</code>	Returns the corresponding country according code to the built-in GeoIP database.

USM Appliance default plugin functions (Continued)

Function	Description
geoip_ getCountryName (addr)	Returns the country name of the location this IP address is in.
geoip_ getLatitude (addr)	Returns the latitude of the location this IP address is in.
geoip_ getLongitude (addr)	Returns the longitude of the location this IP address is in.
geoip_ getMetroCode (addr)	Returns the metro code of the location this IP address is in.
geoip_ getPostalCode (addr)	Returns the postal code of the location this IP address is in.
geoip_ getRegionCode (addr)	Returns the region code of the location this IP address is in.
geoip_ getRegionName (addr)	Returns the region name of the location this IP address is in.
geoip_ getTimeZone (addr)	Returns the timezone of the location this IP address is in.
resolv (host)	Returns the IP address of a host. The lookup is first performed on a local copy of the asset database on the sensor, then the configured resolver (usually DNS) is tried. A host not found will result in a value of 0.0.0.0.
resolv_ip (addr)	Translates an IPv4 address to hostname.
resolv_port (port_ name)	Takes a network service name and returns the port number on which the service is defined by /etc/services.
md5sum (string)	Returns the MD5 hash of a field.
normalize_ protocol (protocol)	Returns protocol information.

USM Appliance default plugin functions (Continued)

Function	Description
<code>normalize_date_american (string_date)</code>	Returns a UNIX epoch date in the American date format.
<code>normalize_date (string_date, american_format=False)</code>	Returns a UNIX epoch date <i>not</i> in the American date format.
<code>upper (string)</code>	Returns a uppercase version of the string supplied.
<code>sanitize (string)</code>	Converts occurrences of "\n" to "\r".

Supported Formats by the `normalize_date()` Function

When the USM Appliance plugins parse logs received from various devices, they use a built-in function, `normalize_date()`, to convert different date formats to ISO 8601, the format accepted by the USM Appliance Server.

The table below shows the date formats that the `normalize_date()` function supports. The `normalize_date()` function compares the date format in the log with the supported formats, in the order presented in this table, until it finds a match.

If the date format of your device is not listed in this table, you can write a custom function to parse it yourself. See [Customize Plugin Date and Time Formats](#) for instructions.

Date Formats supported by `normalize_date()`

Device or Format Name	Example
DC	2/15/2012 12:00:36 PM
Syslog	Oct 27 10:50:46
Apache	29/Jun/2007:17:02:20
Syslog-ng	Oct 27 2007 10:50:46
Bind9	10-Aug-2009 07:53:44
Snare	Sun Jan 28 15:15:32 2007

Date Formats supported by normalize_date() (Continued)

Device or Format Name	Example
Snort	11/08-19:19:06
Suricata-http	03/20/2012-12:12:24.376349
Arpwatch	Monday, March 15, 2004 15:39:19 +0000
Heartbeat	2006/10/19_11:40:05
Netgear	11/03/2004 19:45:46
Tarantella	2007/10/18 14:38:03
Citrix	02/28/2013:12:00:00
OSSEC	2007 Nov 17 06:26:18
IBM	11/03/07 19:22:22
Lucent1	084658,1516697218 (hhmmss,timestamp)
Lucent2	084658+/- (hhmmss+/-)
Lucent3	084658 (hhmmss)
Nagios rrd	1162540224
FileZilla	11.03.2009 19:45:46
HP Eva	2 18 2009 14 9 52
Websense2	11 Jan 2011 09:44:18 AM
Exchange	2011-07-08T14:13:42.237Z
Sonicwall	2011-05-12 07 59 01
CSV	09/30/2011,10:56:11
Honeyd	2011-05-17-09:42:24
Epilog	2011-11-21 06: 15:02
WMI	20180121084344.000000-000
Spanish Date	20120202 12:12:12
SNMPTRAP	Mar 07, 2012 - 08:39:49

Date Formats supported by normalize_date() (Continued)

Device or Format Name	Example
CheckPoint	1Feb2012;0:05:58 or 1Feb2012 0:05:58
Lilian* Date	11270 02:00:16
Bluecoat	2015-08-14 09:30:00
American Date	08/14/15 09:30:00 or 08/14/2015 09:30:00
Fortigate	date=2015-03-17 time=22:03:55
Sophos UTM	2014:09:06-00:00:06
Snare_2	Jan. 22 11:20 AM
Aruba-airwave	01/22/2018 11:20 AM
Anti-Spam SMTP Proxy (ASSP)	01-22-18 11:21:35

*Lilian is the number of days since the beginning of the Gregorian Calendar on October 15, 1582

Create New Plugins Using the Plugin Builder

In addition to the other methods described for customizing or creating new USM Appliance plugins, you can also use the Plugin Builder provided in the USM Appliance web UI to create new custom plugins. The plugin builder provides an interactive smart wizard program that guides you through the process of automatically creating and configuring a new plugin to deploy with the USM Appliance.

Using the Plugin Builder to Create a New Custom Plugin

The Plugin Builder wizard program lets you upload a sample log file which it then uses to identify data to be normalized into USM Appliance event fields for a new plugin.

To Use the Plugin Builder

1. Select the **Configuration > Deployment** option from the USM Appliance web UI.
2. Select the **Plugin Builder** tab.

The USM Appliance web UI displays a list of any custom plugins previously created with the Plugin Builder.



Note: The Plugin Builder display only shows new plugins created using the Plugin Builder. It does not show any other custom plugins that may have been created or customized outside of the Plugin Builder. However, you can locate those plugins by viewing the contents of the USM Appliance plugin configuration folder:

`/etc/ossim/agent/plugins.`

You can also view and enable the custom plugins by establishing an SSH connection to the AlienVault Console and selecting the **Configure Sensor > Configure data source plugin** option from the AlienVault Setup menu.

3. Click the **Add New Plugin** button.

The USM Appliance web UI displays the first step of the Plugin Builder wizard. You are prompted to select a sample log file the Plugin Builder will use to identify data that can be normalized into USM Appliance event fields.

ADD NEW PLUGIN

1 UPLOAD LOG

2 PROPERTIES

3 EVENT TYPES

4 REVIEW

Upload Log File

Step 1: Upload a log file in plain text format to get started.
The Plugin Builder will parse the file to help you create the plugin.

4. Click the **Browse** button to navigate to the location of the sample log file you want to use to identify possible event field mapping.

After you choose a log file, the Plugin Builder determines whether it can upload the file for event field mapping and displays a green checkmark if successful.

5. Click **Next**.

The Plugin Builder advances to step 2 in which you are prompted to enter information about the source of the log file.

ADD NEW PLUGIN

1 UPLOAD LOG

2 PROPERTIES

3 EVENT TYPES

4 REVIEW

Plugin Properties

Step 2: Classify your plugin by adding properties below.

Vendor*

Model*

Version

Product Type*

Select Product Type ▼



Note: Vendor and Model entries may not contain spaces or special characters. Only the plugin ID is included in the plugin configuration filename. Vendor, model, and version information is included into the plugin file header.

- For the Product Type field, select the product type from options displayed in the popup list. (The categories list match the USM Appliance SIEM taxonomy. When you have finished the Plugin Properties entries, click **Next**.

The Plugin Builder now displays the initial mapping of log file entries to USM Appliance event fields for specific named event rules.

Event Types

Step 3: Patterns were normalized for the following events. All events must be categorized for the SIEM using the "Edit" icon. Event properties can also be reviewed and adjusted if necessary. Any event that you would like for Alienvault to ignore should be deleted using the "Trash" icon before creating the plugin.

EVENT NAME	EVENT TYPE	EXTRACTED DATA	STATUS
rule 1	TBD	<p>Log line:</p> <pre>May 16 06:36:25 10.130.199.5 date = 2014-05-16 time = 06:36:25 devname = CHI-FG240D devid = FG240D 4613801196 logid = 0002000012 type = traffic subtype = multicast level = notice vd = Guest-Wifi srcip= 10.130.0.116 src port= 68 srcintf = "Wifi-Switch" dstip= 255.255.255.255 dst port= 67 dstintf = "NonfundSwitch" sessionid = 0 status = deny policyid = 0 dstcountry = "Reserved" srccountry = "Reserved" trandisp = noop service = DHCP proto= 17 duration = 0 sentbyte = 328 rcvbyte = 0 sentpkt = 1 rcvpkt = 0</pre> <p>Tokens:</p> <pre>DATE USERDATA1 date = 2014-05-16 time = 06:36:25 devname = CHI-FG240D devid = FG240D 4613801196 logid = 0002000012 type = traffic subtype = multicast level = notice vd = Guest-Wifi srcip= SRC_IP src port= SRC_PORT srcintf = "Wifi-Switch" dstip= DST_IP dst port= DST_PORT dstintf = "NonfundSwitch" sessionid = 0 status = deny policyid = 0 dstcountry = "Reserved" srccountry = "Reserved" trandisp = noop service = DHCP proto= 17 duration = 0 sentbyte = 328 rcvbyte = 0 sentpkt = 1 rcvpkt = 0</pre>	

The top portion of the display shows data contained in the sample log file you submitted and the bottom portion displays corresponding event field mapping that the Plugin Builder identified for one or more named event rules.

- Click the **Edit** (✎) button.

The Plugin Builder displays a set of fields in which you can edit the name, category (and subcategory) that will be used in USM Appliance when events matching specific rules will be generated by the plugin.

EDIT PATTERN

Edit event properties and map the log line to event fields below.

FILE	rtrutna_20170513000232_fortigate.log	
EVENT NAME	rule 1	
STATUS	Non consolidated	
DATA SOURCE	fortigate fortinet	
CATEGORY	Access	
SUBCATEGORY	Alert	

Edit Tokens

May 16 06:36:25 10.130.199.5 date

0002000012 type = traffic subtype

"Wifi-Switch" dstip= 255.255.255.

dstcountry = "Reserved" srccountr

rcvdbyte = 0 sentpkt = 1 rcvdpkt =

Authentication

Availability

Database

Denial Of Service

Exploit

Honeypot

Info

Inventory

Malware

Network

Policy

Recon

Suspicious

System

Voip

Wireless

name = CHI-FG240D devid = FG240D 4613801196 logid = 0002000012 type =

-Wifi srcip= SRC_IP src port= SRC_PORT srcintf = "Wifi-Switch" dstip=

sessionid = 0 status = deny policyid = 0 dstcountry = "Reserved"

P proto= 17 duration = 0 sentbyte = 328 rcvdbyte = 0 sentpkt = 1

In the area below the event property fields, the Edit Tokens section lets you edit or update data *tokens* assigned or mapped to USM Appliance event fields. You can also map additional unassigned data patterned after the log data and assign those data tokens to new event fields.

- In the Edit Tokens section, clicking on highlighted keywords shows the mapping of token data to assigned event fields. The Plugin Builder shows the current token mapping in a dialog box at the bottom of the display. You can adjust the slider at the bottom to change the token mapping and change other attributes of the event field mapping.
- Clicking on non-highlighted token data in the upper portion of the display lets you create additional log data to event field mappings in the dialog box shown at the bottom of the display.

EDIT PATTERN

CATEGORY

SUBCATEGORY

-- Select a category --

May 16 06:36:25 10.130.199.5 date = 2014-05-16 time = 06:36:25 devname = CHI-FG240D devid = FG240D 4613801196 logid = 0002000012 type = traffic subtype = multicast level = notice vd = Guest-Wifi srcip= 10.130.0.116 srcport= 68 srcintf = "Wifi-Switch" dstip= 255.255.255.255 dstport= 67 dstintf = "NonfundSwitch" sessionid= 0 status = deny policyid= 0 dstcountry = "Reserved" srccountry= "Reserved" trandisp= noop service= DHCP proto= 17 duration= 0 sentbyte= 328 rcvbyte= 0 sentpkt= 1 rcvpkt= 0

DATE USERDATA1

date = 2014-05-16 time = 06:36:25 devname = CHI-FG240D devid = FG240D 4613801196 logid = 0002000012 type = traffic subtype = multicast level = notice vd = Guest-Wifi srcip= SRC_IP srcport= SRC_PORT srcintf = "Wifi-Switch" dstip= DST_IP dstport= DST_PORT dstintf = "NonfundSwitch" sessionid= 0 status = deny policyid= 0 dstcountry = "Reserved" srccountry= "Reserved" trandisp= noop service= DHCP proto= 17 duration= 0 sentbyte= 328 rcvbyte= 0 sentpkt= 1 rcvpkt= 0

SELECTED DATA

status

SIMILAR DATA FOUND

EVENT FIELD

NOT ASSIGNED

FIXED FIELD

True

DO YOU WANT RESIZE THE TOKEN?

May 16 06:36:25 10.130.199.5 date=2014-05-16 time=06:36:25 devname=CHI-FG240D devid=FG240D4613801196 logid=0002000012 type=traffic subtype=multicast level=notice vd=Guest-Wifi srcip=10.130.0.116 srcport=68 srcintf="Wifi-Switch" dstip=255.255.255.255 dstport=67 dstintf="NonfundSwitch" sessionid=0 status=deny policyid=0 dstcountry="Reserved" srccountry="Reserved" trandisp=noop service=DHCP proto=17 duration=0 sentbyte=328 rcvbyte=0 sentpkt=1 rcvpkt=0

You can use the sliding bar at the bottom of the display to adjust the beginning and ending points of data tokens taken from the sample log file that are mapped to event fields.

- Click the Return () link after revising or adding any additional log data you want to map to event fields.
- Click **Save & Close** and then click **Next**.

ADD NEW PLUGIN

1 UPLOAD LOG

2 PROPERTIES

3 EVENT TYPES

4 REVIEW

Review Plugin Info

Plugin File

/custom_plugin_100002.cfg

Vendor

Fortinet

Model

FortigateNG

Version

5

Product Type

Firewall

Number of Event Types

1

FINISH

275

USM Appliance™ Deployment Guide

10. Click the **Finish** button to complete creation of the new plugin.

When you click the **Finish** button, the Plugin builder creates both the configuration (`.cfg`) file and the `.sql` file for the new plugin.

After creating the new plugin, the USM Appliance Plugin Builder wizard returns to the main custom plugins display page where it shows the new plugin you just created.



Note: The current Plugin Builder does not allow re-editing of custom plugins from the USM Appliance web UI. You can, however, open the plugin configuration file directly with a text editor and make additional configuration changes. (Custom plugins are saved in the `/etc/alienvault/plugins/custom` folder.) You can also delete the existing plugin from the Plugin Builder's tabular list view, delete an existing plugin, and then start over to make a new plugin using the Plugin Builder wizard.

Deploying Custom Plugins

You can use custom plugins created with the Plugin Builder the same way as all other plugins, by enabling the plugin for individual assets or on a USM Appliance sensor. After creating a new custom plugin, the plugin configuration file is saved to the USM Appliance Server (for USM Appliance All-in-One) and also distributed to all configured remote or external sensors. The plugin `.sql` file is automatically applied to the USM Appliance Server database. There is no need to copy and run the plugin `.sql` on external sensors, because they do not have a separate database.



Note: Export or manual copying of plugin `.cfg` configuration and `.sql` files is only necessary if you want to deploy a new custom plugin to other USM Appliance installations deployed in your environment. Exporting a new custom plugin only exports the plugin `.cfg` configuration file. So, you will still need to manually download the plugin `.sql` file and apply it to the databases associated with any other USM ApplianceServer installations you have deployed in your environment.

Develop New Plugins from Scratch

This section provides an overview of the process you can follow to create a new plugin, from scratch, directly editing and updating the plugin configuration (`cfg`) and `.sql` files needed to collect and normalize events from specific data sources.

Process of Creating a New Plugin

The following procedure details high level steps in the process of creating a new USM Appliance plugin.

1. Create a `<filename>.cfg` file for the new plugin. You may want to make a copy of an existing .cfg file that is similar to the type of plugin you want to create, to save time.
2. Specify a unique plugin ID (9001 and above) for the plugin and also specify the location of the log file the plugin will read from. The range of values available for user-defined plugins is 9001 to 2147483647, except for the following values, which are also reserved.

90003, 90005, 90007, 90008, 10002, 12001, 19004, 19005, 19006, 20505

3. Create event rules using regular expressions to match events coming in from a source log file.
4. Create the .sql file that specifies the data written to the SIEM database for all events/rules field mapping of extracted data. You may want to make a copy of an existing .sql file that is similar to the new plugin you want to create, and change the fields to describe events defined in the new plugin.
5. Activate the plugin.
6. Import your .sql file to the SIEM database using the following command

```
cat <plugin_name>.sql | ossim-db
```

7. Test the plugin using the USM Appliance web UI to see if events are being detected

Plugin Design Best Practices

AlienVault offers the following recommendations for developing a new or custom plugin.

- Use a log sample as large as possible to identify events and data patterns. This helps to ensure that a sufficient number of data variations have been accounted for.
- Extract data from the log by issuing the command, `grep -v` sequentially until no more data are returned.
- Identify all of the values in the log data that may be included in an event.
- Discard any repeated log data.
- Look for data patterns as a way to group them into categories. One organizing principle might be, for example, having the same data field distribution.

- USM Appliance identifies individual events using a `plugin_sid`, consisting of a serial number. For this reason, you may find that you need to add a translation table section to associate captured data log fields to `plugin_sids`. (See [Creating a Plugin Configuration File](#) for information.)
- Estimate the frequency with which any event type would be generated from the log by counting the number of times each log line repeats.

```
grep <log_line> <logFile> | wc -l
```

- If you have multiple similar log lines, evaluate whether it makes sense to apply a single rule to each, thereby creating two or more unique events, or whether you should create one rule that deals with a group of similar log lines and only creates a single event.


In the latter example, you run the risk of making a rule too complex to be effective, because of the number of matches needed.

- Only capture the fields that will be used for correlation later on.
- You may find that you need to create a more generic rule to capture any events that remain after specific rules have all been applied.
- Choose a pre-check string. The plugin uses this string to search the log line before applying the rule. This acts as a filter to avoid applying the rule to a line that cannot match, improving plugin performance. For an example, see the example following step 3 in [Add a New Rule to a Plugin](#). The fourth statement from the top shows `Pre-check="Teardown"`, followed by the `regex`.
- Order the rules starting with 0001 and finishing with 9999. Create groups numbered 0002, 0003, and so forth, leaving room for future expressions.
- Your rules based on specific matching criteria should always be the lowest numbers and the more generic rules, the highest. This helps avoid event masking, which can occur when USM Appliance loads generic rules before specific rules.

When a log line matches a rule, USM Appliance generates an event and does not match it to any other the rule in the queue.

- The `plugin_sids` in a `sql` file do not need to be continuous. You may insert gaps, if needed, to make the file more maintainable. For instance, you can reserve `Plugin_sids` for each group of event types in the following way
 - 1000 to 1999
 - 2000 to 2999

This method works even if you do not have 1000 different events.

- USM Appliance supports a number of built-in functions to simplify the process of converting information extracted from logs into normalized events. In addition, you can create your own custom functions. (See [Define and Use Custom Functions](#)).
-  **Note:** Be careful if you add a custom function to a plugin or if you access a proprietary database. This can degrade performance if not well designed. Custom plugins might take up to five minutes to appear in the USM Appliance web interface after you add them.

Tutorial: Create a Plugin for Microsoft Exchange

In this tutorial, we use Microsoft Exchange to show how to develop a log plugin. The preferred method of collecting logs from the Exchange Server is through NXLog. See [Microsoft Exchange Server through NXLog](#) for details.

Plugin Development Steps

1. Examine the log file from the data source from which you want to create a plugin. Identify all the types of log messages, as well as messages sharing a common structure, but using different values.
2. Create the `<filename>.cfg` file, either by writing a new file or by copying an existing and similar file, then rewriting it.
3. Give the plugin a numeric ID. (See [Creating a Plugin Configuration File](#) for available values.)
4. Specify the location of the file from which the plugin should read.
5. Write regular expressions to parse individual messages from the log file.
6. Test your regular expressions to see if they perform as they should, using a testing tool such as the one available at regex101.com.
7. Create the `.sql` file by copying an existing and similar `.sql` file. Change the fields to describe events included in the custom plugin.
8. Write the `.sql` file to the SIEM database.
9. Enable the plugin through either the AlienVault Setup menu, the USM Appliance web UI, or a USM Appliance asset. (See [Enable Plugins](#).)
10. Test the plugin by sending logs from the data source to USM Appliance. (See [Verify that an Enabled Plugin Is Working Properly](#).)

Creating a Plugin Configuration File

This task creates a plugin configuration file for a data source called "exchangews," and which uses SNMP for data transfer.

To create a plugin configuration file

1. (Optional) Use an existing plugin as a template for the new one by copying an existing plugin file like `SSH.cfg` and renaming it `exchangews.cfg`.
2. Write the new plugin configuration settings:

- a. Change the `plugin_id` field, using any value in the range from 9001 to 2147483647 except for the following:

90003, 90005, 90007, 90008, 10002, 12001, 19004, 19005, 19006, 20505



Note: Because you have copied `SSH.cfg`, you do not need to create a header. If you created a file from scratch, you would need to create one at this juncture. See [The Plugin File Header](#).

- b. Change location to point to the log file `/var/log/exchangews.log`.
- c. Delete the startup and shutdown fields. These fields are not going to be used. There is no application associated with this plugin.
- d. (Optional) Create a new translation table.

A translation table translates a string to a number so that it can be used as a `plugin_sid`.

```
HELLO=1
MAIL=2
RCPT=3
DATA=4
QUIT=5
xxxx=6
DEFAULT_=9999
```

- e. Create new rules, filling up the fields below.
- f. Create two regular expressions to parse the data, because there are two different formats in the log file.

```
[exchangews - Generic rule]
#2011-10-09 05:00:15 1.1.1.1 36A42160 SMTPSVC1 MEE-PDC 192.168.1.2 0
HELO - +36A42160 250 0 48 13 0 SMTP - - - -
#2011-10-09 05:00:16 1.1.1.1 36A42160 SMTPSVC1 MEE-PDC 192.168.1.2 0
MAIL - +FROM:+<test@sample1.com> 250 0 57 45 0 SMTP - - - -
event_type=event
```

```

regexp="(P<date>\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2})\s(P<src_ip>\IPV4)\s(P<userdata2>\S+)\s(P<hostname>\S+)\s(P<userdata3>\S+)\s(P<dst_IP>\IPV4)\s\d\s(P<type>\w+)"
date={normalize_date($date)}
plugin_sid={translate($type)}
dst_ip={resolve($dst_ip)}
src_ip={resolve($src_ip)}
hostname={$hostname}
userdata2={$userdata2}
userdata3={$userdata3}
[exchangews = Generic rule 2 NCSA Format]
#1.1.1.10 - 1.1.1.9 [11/Oct/2011:13:16:40 -0600] "HELO -?+1.1.1.9 SMTP"
250 46
#1.1.1.10 - 1.1.1.9 [11/Oct/2011:13:16:41 -0600] "MAIL
-?+FROM: +<Keith@testdomain.com> SMTP" 250 46
event_type=event
regexp="(P<src_ip>\IPV4)\s-\s(P<dst_ip>\S+)\s\[ (P<date>\d\d\/\w{3}\\/\d{4}:\d\d:\d\d:\d\d)\s-\d{4}\]\s\"(P<type>\w+)"
date={normalize_date($date)}
plugin_sid={translate($type)}
dst_ip={resolve($dst_ip)}
src_ip={resolve($src_ip)}

```

- g. Check regular expressions with logs inside the file `/var/log/exchangews.log`.

There are several utilities on the Internet to test regular expressions written in Python. It is recommended to use one of these utilities to check that the created regular expressions match the logs.



Note: The location parameter is limited to 100 files.

Creating a Plugin .sql File

The following example shows the plugin .sql file corresponding to the plugin configuration file example.

```

INSERT INTO plugin (id, type, name, description) VALUES (9001, 1,
'exchangews', 'Exchange E-mail Web server');
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name, priority,
reliability) VALUES (9001, 1, NULL, NULL, 'exchangews: HELO' ,3, 2);
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name, priority,
reliability) VALUES (9001, 9999, NULL, NULL, 'exchangews: Generic exchange
event' ,3, 2);

```

Updating the SIEM Database

USM Appliance must store all the plugin IDs and event types in its database before it can store any events. For this reason, if you develop a new plugin and you don't first update the database with that data, the USM Appliance Server drops those events, even though the

plugin is working correctly.

To update the SIEM database

1. Write the changes to the SIEM database:

```
cat exchangeys.sql | ossim-db
```

2. Apply changes in the SIEM:

```
ossim-server restart
```


Update Process

This section covers the following subtopics:

- USM Appliance Updates285
- Update USM Appliance Online 286
- Update USM Appliance Offline290
- Operating System Upgrade in Version 5.8.0295
- Error Codes When Updating from Version 5.8.0 to Version 5.8.x299

USM Appliance Updates

AT&T Cybersecurity strongly recommends that you keep the USM Appliance installation up-to-date and on the same version if you have deployed multiple USM Appliance instances. While USM Appliance are backward-compatible, the difference between versions can cause you to miss security events.

Follow the order below while updating different USM Appliance components.

1. USM Appliance Logger (if any)
2. USM Appliance Server or USM Appliance All-in-One
3. USM Appliance Sensor

By following this order, you ensure that the USM Appliance Server/All-in-One correctly processes any data received from the USM Appliance Sensor, should the update contain any formatting changes.

Similarly, while updating the USM Appliance Enterprise Server, which consists of an Enterprise Server and an Enterprise Database, you must update the Enterprise Server first, followed by the Enterprise Database. In doing so, you ensure that the Enterprise Server understands any database changes the update incurs.

The USM Appliance Product Releases

AT&T Cybersecurity delivers patches containing security updates and defect fixes to existing releases. This sometimes includes updates to the underlying operating system. Customers should not change or update the operating system by themselves, see [Unauthorized Modification of USM Appliance Can Lead to Instability](#) for details.

To find out the details of each product release, see the "New Update: AlienVault <version> has been released" messages in the Message Center or the [USM Appliance release notes](#).

The Threat Intelligence Updates

AT&T Alien Labs™ delivers threat intelligence updates to the USM Appliance platform every week. These updates typically include

- Correlation rules
- Cross-correlation rules
- Network IDS signatures

- Host IDS signatures
- Vulnerability threat database
- Reports



Note: Since the threat intelligence update refreshes the vulnerability threat database used by vulnerability scans, it will not finish if any scan job is running.

To find out the details of each threat intelligence update, check Message Center for the *AlienVault Labs Threat Intelligence Update Summary* messages.

The Plugin Feed Updates

Alien Labs typically delivers a plugin feed update to the USM Appliance platform every two months. These updates usually include

- New plugins
- Fixes to existing plugins
- AlienVault HIDS decoders and rules (USM Appliance version 5.3.2 and later)
- Common Platform Enumeration (CPE) dictionary for plugins

To find out the details of each plugin feed update, check [Message Center](#) for the *Plugins Feed Update* messages.

In USM Appliance version 5.4 and later, you can configure threat intelligence and plugin updates to run automatically. See [Configuring Automatic Updates for Threat Intelligence and Plugins](#) for instructions.

Update USM Appliance Online

You need to update USM Appliance manually after a release becomes available. You can perform the update either from the USM Appliance web UI or the AlienVault Setup menu.

In USM Appliance version 5.4 and later, you can configure threat intelligence and plugin updates to run automatically, but you still need to run the product updates manually.



Important: To ensure performance, based on the [USM Appliance data sheet](#), the update process terminates when you have more than 200 million events in the database.

To download the latest packages, make sure USM Appliance can connect to data.alienvault.com through port 80.


Finding Out the Version of Your USM Appliance

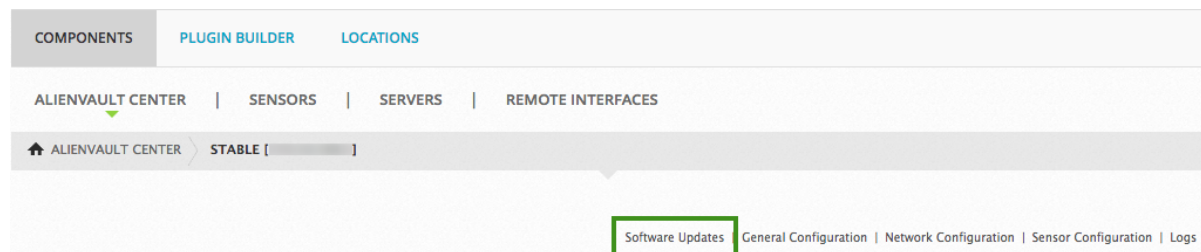
The easiest way to find out the version of your USM Appliance is from the web UI.

To find out the version of your USM Appliance instance

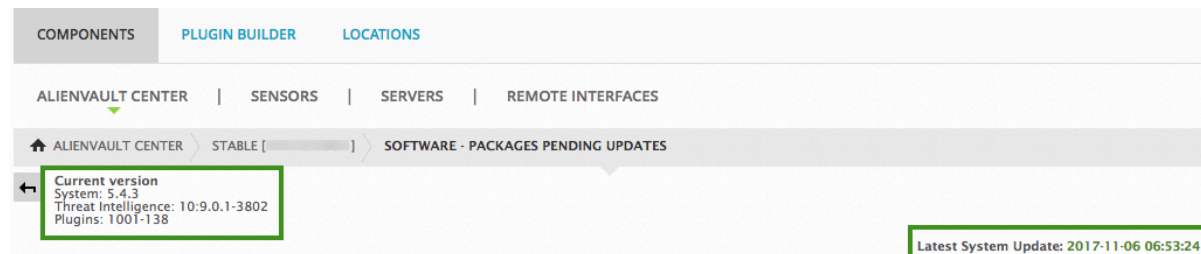
1. Log into the USM Appliance web UI using an account with administrative privileges.
2. Go to **Configuration > Deployment**.

The AlienVault Components Information page displays.

3. Click the  icon of the USM Appliance instance.
4. On the resulting page, click the **Software Updates** link.



The AlienVault Package Information page displays



The pages shows the current version of your system, threat intelligence, and plugins, as well as the date and time of your latest system update.



Note: If your USM Appliance is already on the latest version, the list of AlienVault packages will be empty. You will see "System Updated" instead. If you are not on the latest version, however, the web UI displays the list of packages you can update to.

Updating from the Web UI

You can update USM Appliance from the USM Appliance web UI or the AlienVault Setup menu. AlienVault recommends the web UI for its ease of use.

To update USM Appliance from the web UI

1. Log into the USM Appliance web UI using an account with administrative privileges.
2. Go to **Configuration > Deployment**.

The AlienVault Components Information page displays.

3. Check the **New Updates** column for the USM Appliance component of interest. If an update is available, a downward-pointing arrow icon displays:

DEPLOYMENT					
COMPONENTS SMART EVENT COLLECTION LOCATIONS					
ALIENVAULT CENTER SENSORS SERVERS REMOTE INTERFACES					
ALIENVAULT CENTER					
ALIENVAULT COMPONENTS INFORMATION					
NAME	STATUS	RAM USAGE	SWAP USAGE	CPU USAGE	NEW UPDATES
VirtualUSMAAllinOneLite [192.168.73.159] Server Sensor Web Interface Database	UP	87.70 %	7.60 %	9.55 %	

SHOWING 1 TO 1 OF 1 ENTRIES

FIRST PREVIOUS 1 NEXT LAST

4. To retrieve information about the update, click the arrow.
5. Review the target update packages.
6. Update the software:
 - To update threat intelligence or plugin feeds, click **Update Feed Only**.
 - To upgrade to a new product release, click **Update All**.

The process can take several minutes. The system displays a success message when the update process completes without issues.

Updating from the AlienVault Setup Menu

You can also update USM Appliance from the AlienVault Setup menu. Some updates, especially those that require a system restart, must be run from the AlienVault Setup menu, because the system loses connection to the web UI during a restart. AlienVault will specify, in the release notes, if you need to run the update from the AlienVault Setup menu.

To update USM Appliance from the AlienVault Setup menu

1. Log in to USM Appliance.



Although login via `SSH` is supported, AT&T Cybersecurity recommends using a physically connected monitor and keyboard, or a direct connection via the VMWare or Hyper-V virtual console. If your `SSH` connection is interrupted during the update, your USM Appliance may become irreparably corrupted.

An update pre-check will display a warning if it detects an `SSH` connection before you apply your update.



Note: AT&T Cybersecurity recommends using a direct console connection via the VMWare or Hyper-V management interface, or directly connected keyboard and monitor instead of an `SSH` connection, though both are supported. If your `SSH` connection is interrupted during the update, your USM Appliance may become irreparably corrupted.

An update pre-check will show a warning if it detects an `SSH` connection before you apply your update.

The AlienVault Setup menu appears with **System Preferences** as the default selection.

2. To update the appliance, press **Enter** (<OK>).
3. Tab to **Update AlienVault System** and press **Enter**.
4. Update the software:
 - To update to a new product release, tab to **Update System** and press **Enter**.
 - To update threat intelligence or plugin feeds only, tab to **Update Threat Intelligence** and press **Enter**.
5. Confirm your selection by pressing **Enter**.

The process can take several minutes. The system displays a success message when the update process completes without issues.

When connecting to the USM Appliance instance through a console (not using `SSH`), a reboot is needed after an update. The console then displays a splash screen after the post message and through the boot process. If you wish to see boot messages, you can press the up arrow key to display them, or the down arrow key to return to the splash screen.

Configuring Automatic Updates for Threat Intelligence and Plugins

In USM Appliance version 5.4 and later, you can configure threat intelligence and plugin updates to run at a certain hour every day. USM Appliance will execute the update as it becomes available. You will see a message in the Message Center to confirm the success or failure of the update.



Important: Do not schedule the update to run when a vulnerability scan is in progress, because the update may change the rule the scan uses, causing the scan to fail.

To configure automatic updates

1. Log into the USM Appliance web UI using an account with administrative privileges.
2. Go to **Configuration > Administration > Main**.
3. Click **Automatic Updates**.
4. Change **Automatically run Plugin updates and Threat Intelligence updates** to **Yes**.
5. In **Schedule automatic updates to run**, select the hour for USM Appliance to check (daily) and run the update when available.

The schedule is based on the time zone you have configured for this USM Appliance instance.

Update USM Appliance Offline

Updating your USM Appliance offline requires use of the following items

- A USM Appliance ISO image
- A USB drive with a USB 2.0 interface to burn the ISO image

In order to perform an offline update on AlienVault USM Appliance, you first need to download the ISO image of the version you desire. For instructions, see [Download a USM Appliance ISO Image](#).

Then you need to burn the ISO image to a USB drive. For instructions, see [Burn the USM Appliance ISO Image to a USB Drive](#).

Using an ISO image burned to a USB drive is the preferred way to update USM Appliance offline. However, the USM Appliance VMware image does not contain a USB controller, therefore you cannot connect a USB drive to it. For instructions on how to add a USB controller in a virtual machine, see [VMware's knowledge base article about USB support](#).

If using a USB drive is not an option, you can upload the ISO image to a datastore and then access it through a CD or DVD drive. Click the following links for instructions from VMware documentation respectively

- [Upload ISO Image Installation Media for a Guest Operating System](#)
- [Add a CD or DVD Drive to a Virtual Machine in the vSphere Web Client](#)



Note: Select "Datastore ISO File" as the device type and "Connect At Power On" to connect the device when the virtual machine turns on.

Finally, you can follow the procedure below to update your USM Appliance.



Important: To ensure performance, based on the [USM Appliance data sheet](#), the update process terminates when you have more than 200 million events in the database.

To update the USM Appliance offline

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 **Update AlienVault System**.
4. Select **Update (Offline)**.
5. Insert the USB drive into the machine now, or connect the CD/DVD drive with the USM Appliance ISO image, and then press **Enter** (<OK>).

The update process scans for any connected file system, either USB or CD/DVD, and mounts it automatically.

Download a USM Appliance ISO Image

In order to perform an offline update or software restoration on AlienVault USM Appliance, you first need to download the ISO image of the version you desire.

- For offline update downloads, visit <https://offlineupdate.alienvault.com/files/>.
- For software restoration downloads, visit <https://offlineupdate.alienvault.com/images/>.

To download the USM Appliance ISO image

1. Go to the corresponding download site based on your need.
2. Enter the license key for the product you try to download.
3. Click **Submit**.
4. Locate the USM Appliance version you want to download and click the link.



Note: The offline update download file starts with "AlienVault_USM_UPDATE-FOR-64bits." The software restoration download file starts with "USB_Restoration."

5. Verify your download by comparing its MD5 checksum against the one listed in the `md5.txt` file, available on the same site.



Warning: Running an antivirus scan on the downloaded image will produce hundreds of false positives due to the virus and malware signatures included in NIDS.

Next ...

For instructions on offline update, see [Update USM Appliance Offline](#).

For instructions on software restoration (factory reset), see [Restore Software on a USM Appliance Hardware](#).

Burn the USM Appliance ISO Image to a USB Drive

This procedure is a prerequisite to updating USM Appliance offline or restoring the software on a hardware appliance to its factory settings. For details, see [Update USM Appliance Offline](#) or [Restore Software on a USM Appliance Hardware](#).



Important: This process deletes all files stored on the USB device.

The procedure is different based on the operating system you use. Follow the steps accordingly.

Linux

To burn the ISO image from a Linux machine

1. Insert the USB drive into the USB port on your computer.
2. To copy the ISO image, open a terminal and run the following command

```
sudo dd if=<USM_image.iso> of=<USB_device> bs=4M
```


Replace `<USM_image.iso>` with the full path of the downloaded ISO image file, and `<USM_device>` with the USB device location.

For example, if you save the image file in `/home/user/temp/image.iso` and the USB device location is `/dev/sdb`, the command would be

```
sudo dd if=/home/user/temp/image.iso of=/dev/sdb bs=4M
```

3. Eject the USB device.

Mac OS X

To burn the image from a Mac OS X machine

1. Insert the USB drive into the USB port on your computer.
2. To list the devices connected to your computer, open a terminal and run the following command

```
diskutil list
```

3. To identify the USB device, look for **DOS_FAT_32** as the disk type.

The location of the USB device in the following illustration is `/dev/disk1`.

```
MacBook-Pro-de-Jose-Miguel:~ Jose-Miguel$ diskutil list
/dev/disk0
#          TYPE NAME              SIZE       IDENTIFIER
0:        GUID_partition_scheme   *500.3 GB   disk0
1:          EFI                   209.7 MB    disk0s1
2:      Apple_HFS Macintosh HD     499.4 GB    disk0s2
3:      Apple_Boot Recovery HD     650.0 MB    disk0s3
/dev/disk1
#          TYPE NAME              SIZE       IDENTIFIER
0:        FDisk_partition_scheme   *2.0 GB     disk1
1:          DOS_FAT_32 UNAME        2.0 GB     disk1s1
```

4. Before burning the image, unmount your USB device

```
diskutil unmountDisk <USB_device_location>
```

Following the example in above, the command would look like this

```
diskutil unmountDisk /dev/disk1
```

5. Copy the image

```
sudo dd if=<USM_image.iso> of=<USB_device> bs=1m
```

Where

- <USM_image.iso> is the full path of the ISO image file.
- <USM_device> is the USB device location.

For example, if you save the image file in `/home/user/temp/image.iso` and the USB device location is `/dev/disk1`, the command would be:

```
sudo dd if=/home/user/temp/image.iso of=/dev/disk1 bs=1m
```

6. Eject the USB device

```
diskutil eject <USB_device>
```

Windows

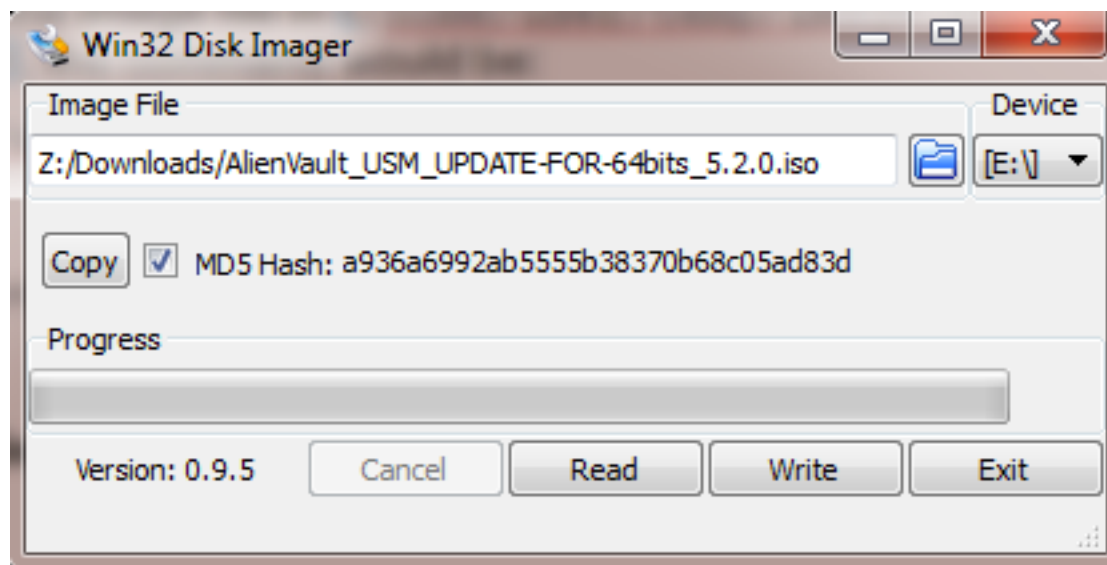
To burn the image from a Windows machine

1. Insert the USB drive.
2. If you haven't already, download [Win32 Disk Imager](#) from SourceForge and install it on your computer.

Win32 Disk Imager is a tool for writing images to USB drives.

3. Launch Win32DiskImager and select the image file.

Win32 Disk Imager populates the **Device** field with the USB drive automatically.



4. To verify that the ISO image is the correct one, select **MD5 Hash**.

Win32 Disk Imager checks the image file and displays its MD5 checksum. Confirm that it matches the one received from Support.

5. Click **Write**.

Confirm while prompted.

6. Exit Win32 Disk Imager after the progress completes.
7. Eject the USB drive.

Operating System Upgrade in Version 5.8.0

USM Appliance version 5.8.0 includes an operating system (OS) upgrade to improve the performance and security of your deployment. The upgrade process consists of three parts:

- **Perform Pre-Checks:** Runs a set of diagnostic checks to ensure that your deployment meets AT&T Cybersecurity's requirements.
- **Update OS Packages:** Brings the OS packages to the designated versions.
- **Update USM Appliance Packages:** Brings the USM Appliance specific packages to the designated versions.

The upgrade process aborts if any of the pre-checks fail. The following table lists the various errors you may receive. If you need help passing these checks, please contact [AT&T Cybersecurity Technical Support](#).

Pre-Check Error Codes and Messages

Error Code	Error Message
1	alienvault-update is already running ... exiting.
2	System cannot be updated because a vulnerability scan is currently running. Try again later.
3	The system must be rebooted. Please, reboot the system before starting the update process.
4	The verification process could not be completed. Signature file not found.
5	The verification process could not be completed. Signature is invalid.
6	System cannot connect to APT. Execute 'dpkg --configure -a --force-confnew' to correct the problem.
22	Unable to obtain database password. Please, check your ossim_setup.conf file.
23	mysqlcheck command not found.

Pre-Check Error Codes and Messages (Continued)

Error Code	Error Message
24	Your database is corrupted and cannot be repaired.
27	It seems that there are more than 200M events in the database or your indexes are corrupted.
29	Cannot change repositories.
31	Error downloading packages.
32	Error while updating a major version.
33	Error while updating a major version (MariaDB cannot be installed).
34	Error while updating a major version (Squid cannot be installed).
35	ossim_setup.conf has been removed. Try to recover a backup from /etc/ossim/.
36	Error updating sources list.
40	Dash shell cannot be installed.
42	AlienVault preseeds cannot be set.
50	Parsing error: Some command line arguments are unknown. Please, type alienvault-update --help for more information.
51	System must be running v5.7.6 to perform an OS update.
52	System is unstable, some packages are not correctly installed and configured.
53	Your system does not meet the minimum requirements (For more information, review https://cdn-cybersecurity.att.com/docs/data-sheets/usm-appliance.pdf).
54	Your system has less partitions than required in /dev/sda, please contact with support.
55	System is running in HA mode. If you want to update your system, please disable the HA system by running alienvault-ha-assistant -d, and then update.
56	CPU usage is above 90%, the OS update requires CPU usage to be below the threshold.
57	USM Appliance cannot be updated, packages cannot be installed.
58	No profiles found in your system.
59	ossim_setup.conf is corrupted. Profiles not found. Try to recover a backup from /etc/ossim/."

Pre-Check Error Codes and Messages (Continued)

Error Code	Error Message
60	The command apt-get update failed. Please, check your internet connection.
61	You don't have enough disk space. Please, free up space on your hard drive.
62	A problem occurred checking your USM Appliance license. Please, check the update log for more information.
64	Database schema version mismatch.
65	Packages cannot be downloaded. Please, check the update log for more information.
66	Failed to install package from Threat Intelligence update.
67	Apt command cannot be updated
68	System is unstable, some packages have not been updated to the latest version.
69	bash script was executed isolatedly. Please, use alienvault-update command instead.
70	MySQL cannot be started.

You may also receive some warnings from running these pre-checks. See the following table for details. AT&T Cybersecurity recommends that you review the warning messages and correct as many issues as possible, but you can proceed with the upgrade by entering **y** when the system asks if you want to continue.

Pre-Check Warnings

Number	Warning Message
1	SSH Session detected. AlienVault recommends updating the system from a terminal to prevent possible connection problems during the update.
2	The verification process could not be completed. User agent signature is invalid.
3	There is no connection. UserAgent will not be downloaded.
4	apt-get --yes autoremove --purge could not be executed.
5	Failed to install libhyperscan!

Pre-Check Warnings (Continued)

Number	Warning Message
6	No event backup with less than 14 days found. It's recommended creating a new backup and copying it to an external device.
7	No configuration backup with less than 14 days found. It's recommended creating a new backup and copying it to an external device.
8	NfSen backup cannot be created.
9	MySQL backups cannot be created.
10	MySQL backups cannot be restored.
11	Default api periodic tasks cannot be enabled.
12	Default api periodic tasks cannot be disabled.
13	New Squid configuration cannot be applied.
14	Squid backup cannot be created.
15	Squid backup cannot be restored.
16	Nagios module cannot be disabled in Apache server.
17	Nagios module cannot be enabled in Apache server.
18	More than 3 partitions has been detected in /dev/sda. It's recommended contacting with support before proceeding.

Because USM Appliance needs to reboot during the OS upgrade, you cannot perform this particular update from the browser. For the same reason, it is not recommended to run the upgrade from an `SSH` session either. Please run the update from a terminal or a virtual machine (VM) console.

To upgrade the OS

1. Launch the AlienVault Console and use your credentials to log in.

The AlienVault Setup menu displays.

2. Select **System Preferences**.
3. Select **Update AlienVault System**.

4. Select **Upgrade Operating System** or **Upgrade Operating System (Offline)**, and then press **Enter**. If choosing offline, see [Update USM Appliance Offline](#) on how to prepare the ISO image.



Important: These two options are only available in USM Appliance version 5.7.6.

5. Confirm your selection by pressing **Enter**.

The upgrade process starts, writing its progress to

`/var/log/alienvault/update/alienvault57to58-update-<timestamp>.log`. For example:

```
## Alienvault-update starting on 2020-02-18 21:56:05
## logging to /var/log/alienvault/update/alienvault57to58-update-1582062965.log

mount: /dev/sr0 is write-protected, mounting read-only
-- Running system prechecks
-- Checking apt status
-- Performing update prechecks
-
```

You can check the log file periodically to monitor the progress. This upgrade can take more than 30 minutes to finish.

Error Codes When Updating from Version 5.8.0 to Version 5.8.x

To ensure that your deployment meets AT&T Cybersecurity's requirements, USM Appliance runs a set of diagnostic checks before updating to a new version. The update process aborts if any of the pre-checks fail.

The following table lists the various errors you may receive when updating from USM Appliance version 5.8.0 to later versions. (If you are updating from version 5.7.6 to 5.8.0, see the error codes in [Operating System Upgrade in Version 5.8.0](#) instead.) Should you need help passing these checks, please contact [AT&T Cybersecurity Technical Support](#).

Pre-Check Error Codes and Messages

Error Code	Error Message
1	alienvault-update is already running ... exiting.
2	System cannot be updated because a vulnerability scan is currently running. Try again later.
3	The system must be rebooted. Please, reboot the system before starting the update process.
4	The verification process could not be completed. Signature file not found.
5	The verification process could not be completed. Signature is invalid.
6	System cannot connect to APT. Execute 'dpkg --configure -a --force-confnew' to correct the problem.
7	Missing or wrong permissions in update script or errors in JSON.
22	Unable to obtain database password. Please, check your ossim_setup.conf file.
23	mysqlcheck command not found.
24	Your database is corrupted and cannot be repaired.
27	It seems that there are more than 200M events in the database or your indexes are corrupted.
31	Error downloading packages.
32	Error while updating a major version.
35	ossim_setup.conf has been removed. Try to recover a backup from /etc/ossim/.
40	Dash shell cannot be installed.
50	Parsing error: Some command line arguments are unknown. Please, type alienvault-update --help for more information.
52	System is unstable, some packages are not correctly installed and configured.
53	Your system does not meet the minimum requirements (For more information, review https://cdn-cybersecurity.att.com/docs/data-sheets/usm-appliance.pdf).
54	Your system has less partitions than required in /dev/sda, please contact with support.
55	System is running in HA mode. If you want to update your system, please disable the HA system by running alienvault-ha-assistant -d, and then update.

Pre-Check Error Codes and Messages (Continued)

Error Code	Error Message
56	CPU usage is above 90%, the OS update requires CPU usage to be below the threshold.
57	USM Appliance cannot be updated, packages cannot be installed.
59	ossim_setup.conf is corrupted. Profiles not found. Try to recover a backup from /etc/ossim/."
60	The command apt-get update failed. Please, check your internet connection.
61	You don't have enough disk space. Please, free up space on your hard drive.
62	A problem occurred checking your USM Appliance license. Please, check the update log for more information.
64	Database schema version mismatch.
68	System is unstable, some packages have not been updated to the latest version.
69	bash script was executed isolatedly. Please, use alienvault-update command instead.
71	No valid repositories found to perform the update.
72	Error updating kept packages.
73	Error purging packages.
74	There is no update available.
99	Error file (/usr/share/ossim-installer/temp/update-errors.json) cannot be found in the system.

You may also receive some warnings from running these pre-checks. See the following table for details. AT&T Cybersecurity recommends that you review the warning messages and correct as many issues as possible, but you can proceed with the upgrade by entering **y** when the system asks if you want to continue.

Pre-Check Warnings

Number	Warning Message
1	SSH Session detected. AlienVault recommends updating the system from a terminal to prevent possible connection problems during the update.
4	apt-get --yes autoremove --purge could not be executed.
5	Failed to install libhyperscan!
6	No event backup with less than 14 days found. It's recommended creating a new backup and copying it to an external device.
7	No configuration backup with less than 14 days found. It's recommended creating a new backup and copying it to an external device.
11	Default api periodic tasks cannot be enabled.
12	Default api periodic tasks cannot be disabled.
18	More than 3 partitions has been detected in /dev/sda. It's recommended contacting with support before proceeding.

Backup and Restoration

AlienVault USM Appliance does not offer a tool to back up or restore the entire system collectively. However, you can back up or restore your data and system configurations separately. You can also restore the USM Appliance hardware appliance to its factory status if needed.

If you need to transfer backup files from one USM Appliance to another, for example, from a defective USM Appliance to its RMA (Return Merchandise Authorization) replacement, you can use either an SFTP client on Windows, such as WinSCP; or the SCP protocol on Linux.

Topics covered in this section includes the following:

Back Up and Restore Alarms	305
Back Up and Restore Events	308
Back Up and Restore MongoDB	311
Back Up and Restore NetFlow Data	313
Back Up and Restore Raw Logs	316
Back Up and Restore System Configuration	319
Migrate Your USM Appliance Deployment	327
Restore Software on a USM Appliance Hardware	333
Update Your AlienVault License Key	339

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
```

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.

ADMINISTRATION

USERS MAIN BACKUPS

EVENTS | CONFIGURATION

VIEW BACKUP LOGS

BACKUP MANAGER

DATES TO RESTORE

DATES IN DATABASE

23-06-2016
22-06-2016
21-06-2016
20-06-2016
19-06-2016
18-06-2016
17-06-2016

07-06-2016

- All Users -
- All Entities -

RESTORE

CLEAR SIEM DATABASE

LATEST BACKUP EVENTS

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:

VIEW BACKUP LOGS ✕

Showing the latest logs

DATE	BACKUP TYPE	STATUS <input type="text" value="All"/>	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
<div>-- NONE --</div> <div> <input type="text" value="- All Users -"/> <input type="text" value="- All Entities -"/> </div> <div>RESTORE</div>	<div> 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 </div>

Back Up and Restore MongoDB

MongoDB is a cross-platform and open-source document-oriented database, a kind of NoSQL database. As a NoSQL database, MongoDB avoids the relational database's table-based structure to adapt JSON-like documents that have dynamic schemas, which it calls BSON.

This makes data integration for certain types of applications faster and easier. MongoDB is built for scalability, high availability, and performance from a single server deployment to large and complex multi-site infrastructures.

Backing Up MongoDB

To back up MongoDB

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. Back up the MongoDB database and create the dump directory:

```
mongodump --host localhost
```

5. Compress the file:

```
tar cvfz alienvault-mongodb-`date +%s`.tgz dump
```

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

6. Remove the dump directory:

```
rm -rf ./dump
```

This procedure creates the `alienvault-mongodb-<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 MongoDB

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 MongoDB

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 file:

```
tar xvzf alienvault-mongodb-<timestamp>.tgz
```

6. Restore the backup file

```
mongorestore --db inventory dump/inventory
```

7. Remove the dump directory:

```
rm -rf ./dump
```

8. Restart all services for changes to apply:

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

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.

The screenshot shows the 'ADMINISTRATION' section with tabs for 'USERS', 'MAIN', and 'BACKUPS'. The 'BACKUPS' tab is active, showing a 'BACKUP' configuration page. The page title is 'Backup configuration: backup database, directory, interval'. The configuration table is as follows:

Configuration Item	Value	Help Icon
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
```

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		?

- 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

- Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
- 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.

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
```

Back Up and Restore System Configuration

In USM Appliance, you can back up and restore system configurations including system profile, network configuration, inventory data, policies, plugins, correlation directives and other basic settings. You can restore the configurations on a different USM Appliance system from a backup file through the AlienVault Console. You can also manage the configuration backups from the USM Appliance web user interface (UI).



Note: It is not possible to upgrade from AlienVault OSSIM® to USM Appliance, but you can restore AlienVault OSSIM configurations to USM Appliance or vice versa if they are the same version.

Each configuration backup file contains the following, which does *not* include events, alarms, or raw logs:

- Asset and inventory data
- Correlation directives
- Host-based intrusion detection system (HIDS) configurations
- HIDS local rules
- Iptables configurations
- Plugins (both default and customized)
- Policies
- Syslog and logrotate configurations
- System configuration (including network interfaces, system profile, and USM Appliance basic configuration settings)
- Tickets created in USM Appliance
- Virtual private network (VPN) configurations (including VPN certificates)



Important: Be aware that if your VPN certificate changes after the backup has taken place, you must [reconfigure the VPN connection](#) after restoring the backup file.

Backing Up Configurations


By default, USM Appliance backs up the system configurations at 7:00 am local time every day. These display as "Auto" under the Type column in the web UI. You can also manually run a backup at any time.

USM Appliance stores its configuration backup files locally, in the following location:

```
/var/alienvault/backup/configuration_<hostname>_<timestamp>.tar.gz
```

For example, configuration_VirtualUSMAllInOne_1429616586.tar.gz

The integer string represents epoch time, therefore, the backup with the highest number denotes the most recent one. USM Appliance maintains 10 backups on each system, based on their time stamp.

 **Note:** AlienVault recommends keeping a copy of the latest backup file outside of USM Appliance because you may not be able to retrieve these backup files when the system is down.

Before starting the backup, USM Appliance verifies the following:


- No re-configuration process is running.
- No other backup or restore processes are running.
- Sufficient disk space exists to restore the configuration backup.

USM Appliance aborts the backup process if any of these checks fails.

Starting from version 5.2.5, USM Appliance will not generate any configuration backups, automatic or manual, until you set a password to encrypt the backup files. And you need to provide the same password to decrypt the file before a restoration.

To set up a password to encrypt the backup files

1. In the web UI, go to **Configuration > Administration > Main > Backup**.
2. In **Password to encrypt backup files**, type a password between 7 and 32 characters.

 **Important:** Do not use the following characters in your password:
 ; , | , & , \$, < , > , \ n , (,) , [,] , { , } , ? , * , ^ , \ .

3. Click **Update Configuration**.

To run a backup manually

1. In the web UI, go to **Configuration > Administration > Backups > Configuration**.
2. Click **Run Backup Now**.

A message appears showing when the last backup was run and asking if you want to continue.

3. Select **Yes** to start the backup.

These backups display as "Manual" under the Type column.

To see any error messages in the backup logs

1. Go to **Configuration > Administration > Backups > Configuration**.
2. Click **View Backup Logs**.

Backing Up a Child Server from the Federated Server

In a federated environment, where you have USM Appliance Sensors reporting to a USM Appliance Server (child), which then reports to another USM Appliance Server (federated), keep the following in mind:

- Each USM Appliance Server (whether a child or federated server) only triggers automatic backups of itself and directly connected sensors. In other words, the federated server does not trigger automatic backups to its child servers.
- Each USM Appliance stores its own backup file.

You can select the child server on the federated server, but not the reverse. You can run a manual backup of the child server from the federated server by following the standard backup procedure.

To back up the child server from the federated server:

1. Go to **Configuration > Administration > Backups > Configuration**.
2. Choose which system you want to use by expanding **Show Backups for**.
3. Click **Run Backup Now**.

Restoring Configuration Backups

You can only restore a USM Appliance system from a backup file through the AlienVault Console.

Before running a restoration, USM Appliance verifies the following and aborts the restoration process if any of these checks fails:

- No re-configuration process is running.
- No other backup or restore processes are running.
- The backup profile matches the system profile. In other words, you cannot restore a backup file from the USM Appliance Server on the USM Appliance Sensor.
- Backup file version is the same as the target system. In other words, you can only restore a USM Appliance version 5.4.3 backup on a system that is running USM Appliance version 5.4.3.



Note: You can restore an AlienVault OSSIM backup on a USM Appliance or vice versa, as long as they are the same version.

- Sufficient disk space exists to restore the configuration backup.

Before restoring a backup file, you must transfer the file to the target system and place it in the `/var/alienvault/backup/` directory. You can use either an SFTP client on Windows, such as WinSCP; or the SCP protocol on Linux.

To restore a backup file

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 **Backups**.
4. Select **Restore configuration backup**.
5. Select the backup file you want to restore, click **<OK>** or press Enter.
6. Select **<Yes>** to continue.
7. Enter the password used to encrypt the backup files.

The restoration process starts.

After the process finishes, the system restarts automatically.



Note: Your `SSH` connection will drop if the IP address of USM Appliance changes as a result of the restoration.

8. Log in to display the AlienVault Setup menu again.
9. Select **System Preferences**.
10. Select **Reset AlienVault API Key**.

To find out more, see [Reset the AlienVault API Key](#).

Managing Configuration Backups

You can manage the configuration backups on **Configuration > Administration > Backups > Configuration**.

The configuration backups display in a table format.

Columns / fields for configuration backups

Column / Field Name	Description
System	System chosen for backup
Date	Date and time when the backup was run.
Backup	Backup category. Currently the only category is <i>Configuration</i> .
Type	Backup Type. Supported values are <i>Auto</i> and <i>Manual</i> .
Version	Version of the USM Appliance system.
Size	Size of the backup file.
Download	Saves the backup file to your local machine.


By default, USM Appliance sorts the backups by their time stamps, with the latest one at the top.

To look for a backup

- Use the search box at the upper left corner.

Search fields are System (name or IP address), Date, or Type.

To download backups and store them locally


1. Locate the backup you'd like to download.
2. In the last column, click the download icon ().

Sample backup file format:

```
configuration_VirtualUSMAllInOne_1429616586.tar.gz
```

Because the integer string represents epoch time, the backup with the highest number denotes the most recent one.

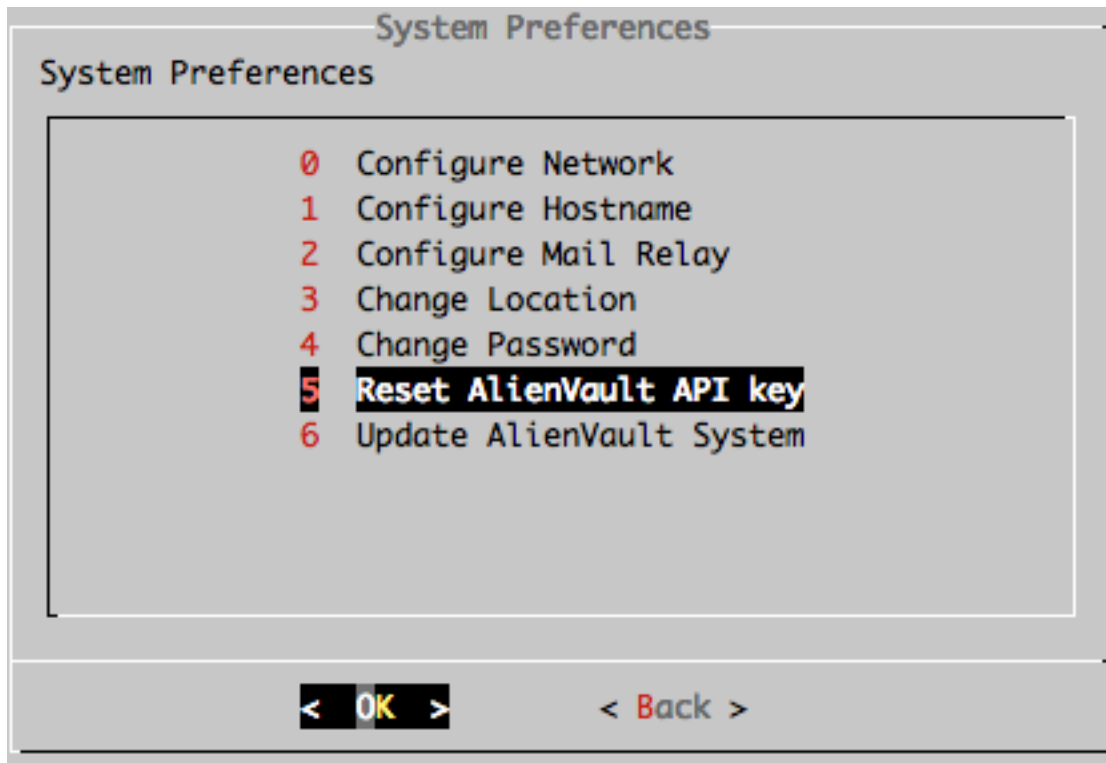
To delete one or more backups

1. Select the backups by checking the square(s) to the left of each backup.
2. Click the delete icon () above the table towards the right.

Reset the AlienVault API Key

Starting from version 5.2.5, USM Appliance and AlienVault OSSIM® offer the option to reset the AlienVault API key from the AlienVault Setup menu.

This option is available in all version 5.2.5 appliances by connecting through `SSH` and selecting **System preferences > Reset AlienVault API key**:



What Is the Reset AlienVault API Key Option for?

In USM Appliance version 5.2.4 and previous releases, AlienVault includes the API key in the configuration backups in clear text. If the backup was downloaded and stored in an insecure location, it could be used to `SSH` into USM Appliance as the `avapi` user and potentially harm the system.

In USM Appliance version 5.2.5 and later releases, the AlienVault API key is no longer included in the configuration backup. Since the `avapi` user performs many critical tasks in USM Appliance, we recommend that you reset the API key in every appliance if you have updated USM Appliance from a previous version.

Resetting the AlienVault API Key in Different Scenarios

You can reset the AlienVault API key at any stage after you have updated to USM Appliance version 5.2.5 or later.

On Isolated USM Appliance All-in-One or USM Appliance Standard Server

This operation is immediate. There is no need to provide `root` password as it is a local change.

Just select the option from the AlienVault Setup menu and select **Yes** when prompted to regenerate the new AlienVault API Key.

In a Distributed Deployment with More Than One USM Appliance Server or USM Appliance Sensor

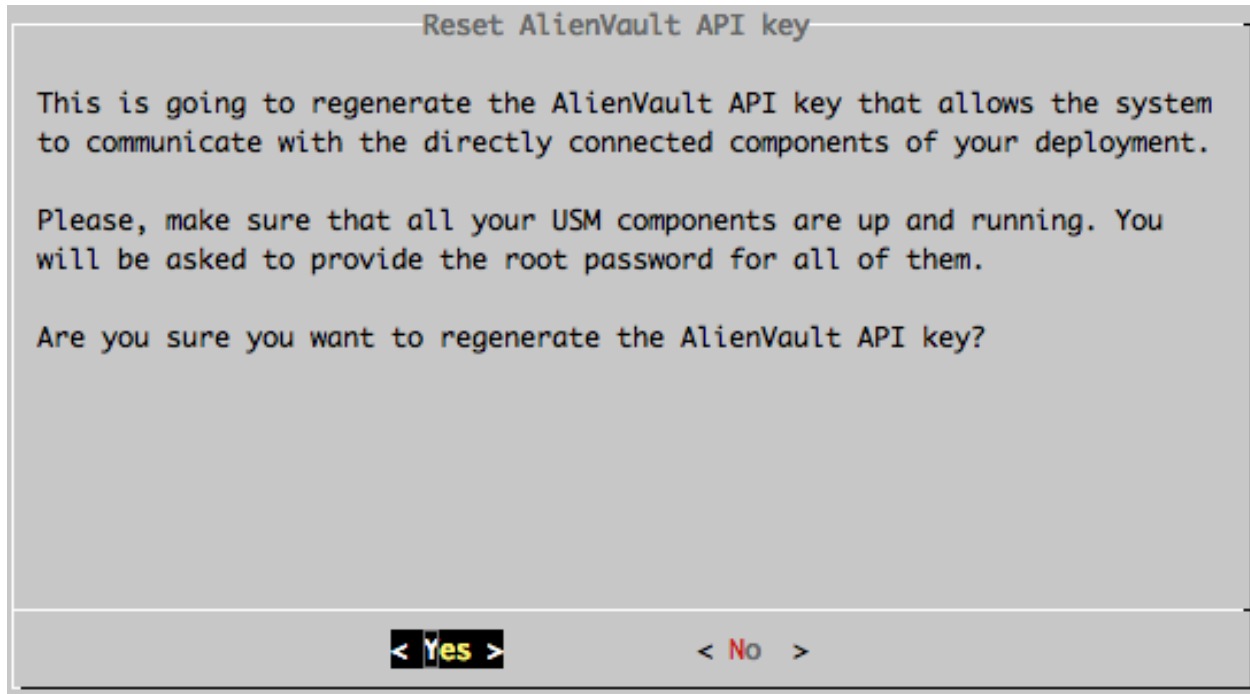
This operation should be executed in **all** USM Appliance instances in order to fully reset the AlienVault API Key.

This should be executed from **bottom-up** considering the deployment hierarchy, in other words, USM Appliance Sensors first, followed by USM Appliance Servers or USM Appliance All-in-Ones, followed by Federated Servers or USM Appliance Loggers.

The reasoning behind this is because choosing "Reset AlienVault API Key" will rewrite the `authorized_keys` file completely. Thus, after resetting API key on a USM Appliance Sensor, it will no longer have the corresponding USM Appliance Server's key, therefore the USM Appliance Server will not be able to communicate with the USM Appliance Sensor through the AlienVault API. But if you reset the AlienVault API key on the USM Appliance Server next, the USM Appliance Server sends it's new key to the USM Appliance Sensor thus restoring the API connectivity.



Note: In distributed deployments, where you have more than one USM Appliance deployed, ensure that you know the password of the `root` user to the directly connected appliances as they are required to reset the AlienVault API keys.



Migrate Your USM Appliance Deployment

In some scenarios, such as disaster recovery, upgrades, or platform changes, you may choose to move your deployed USM Appliance to a new platform or deployment.

You need to apply a new license when migrating from one USM Appliance hardware to another, such as a RMA. The replacement license key will be provided when the new hardware ships.

If you are migrating from a USM Appliance hardware to a virtual machine, or from one virtual platform to another (VMware to Hyper-V or VMware to AWS), the license may only need to be reset. In such cases you can contact [AlienVault Support](#) to obtain the appropriate image, and have your license reset so that it can be applied to the new installation.

Migrating your USM Appliance deployment consists of two tasks:

Backing up Your Current USM Appliance Deployment

USM Appliance does not provide a tool to back up the system as a whole. You need to back up your data and system configurations separately, and then transfer them to the other USM Appliance deployment for restoration.

To back up your USM Appliance deployment

1. Generate a configuration backup from the web UI. For instructions, see [Backing Up Configurations](#).



Note: You need to perform the following steps from the command line, through the AlienVault Console.

2. Connect to the AlienVault Console through `SSH` and use your credentials to log in.
The AlienVault Setup menu displays.
3. 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.
4. 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.

5. 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
```

6. 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.

7. Back up the events:



Note: The example below illustrates how to transfer files from USM Appliance to a machine on your network. If you have the new USM Appliance instance already deployed, you can transfer the files to the new system directly.

This step involves two parts:

- a. Back up the events in the database:

```
mysqldump -p`grep ^pass /etc/ossim/ossim_setup.conf | sed 's/pass=/'`
--no-autocommit --single-transaction --databases alienvault_siem | pigz
> alienvault-events-`date +%s`.sql.gz
```

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

- b. Using the rsync protocol, transfer the old events to the destination:

Syntax:

```
rsync -av --progress /src_folder_path <username>@<dest_ip_
address>:<dest_folder_path>
```

Example:

```
rsync -av --progress /var/lib/ossim/backup
root@10.10.10.10:/var/lib/ossim
```



Important: Leave out the trailing slash ('/') on the source so that the corresponding directory will be created at the destination.

8. Back up MongoDB:

- a. Back up the MongoDB database and create the dump directory:

```
mongodump --host localhost
```

- b. Compress the file:

```
tar cvfz alienvault-mongodb-`date +%s`.tgz dump
```

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

- c. Remove the dump directory:

```
rm -rf ./dump
```

9. Back up NetFlow Data, if using:

```
tar czf alienvault-netflow-`date +%s`.tgz /var/nfsen /var/cache/nfdump
```

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

10. Back up the Raw Logs:



Note: The example below illustrates how to transfer files from USM Appliance to a machine on your network. If you have the new USM Appliance instance already deployed, you can transfer the files to the new system directly.

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.

11. At this step, you have produced the following files:

```
/root/alienvault-alarms-<timestamp>.sql.gz  
/root/alienvault-events-<timestamp>.sql.gz  
/root/alienvault-mongodb-<timestamp>.tgz  
/root/alienvault-netflow-<timestamp>.tgz
```

You should also have a file similar to below generated by the configuration backup:

```
/var/alienvault/backup/configuration_<hostname>_<timestamp>.tar.gz
```

12. Transfer all backup files to your new USM Appliance deployment or an interim system. You can use either an SFTP client on Windows, such as WinSCP; or the SCP protocol on Linux.

Restoring USM Appliance in the New Deployment

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.



Important: If you are restoring USM Appliance to a different platform such as from VMware to Hyper-V, you must acquire a new license. Please contact [AlienVault Support](#) for your request.

To restore your USM Appliance deployment

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. Restore the events:

- a. Restore events into the database:

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

- b. If not done already, use the `rsync` protocol to transfer the event backup files to `/var/lib/ossim` directory.

- c. Change permission on event backup files:

```
chown root:alienvault /var/lib/ossim/backup
chown root:root /var/lib/ossim/backup/*
```

7. Restore MongoDB:

- a. Extract the file:

```
tar xvzf alienvault-mongodb-<timestamp>.tgz
```

- b. Restore the backup file

```
mongorestore --db inventory dump/inventory
```

- c. Remove the dump directory:

```
rm -rf ./dump
```

8. Restore NetFlow data, if using:

- a. Extract the backup file into the '/' directory:

```
tar xvzf alienvault-netflow-<timestamp>.tgz -C /
```

- b. 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
```

9. Restore Raw Logs:

- a. If not done already, use the `rsync` protocol to transfer the raw logs to `/var/ossim/logs` directory.

- b. 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
```

- c. 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
```

10. Restore system configurations:

- a. Copy or move the configuration backup file to the `/var/alienvault/backup` directory.
- b. Type `exit` and then press Enter to return to the AlienVault Setup menu.
- c. Select **Maintenance & Troubleshooting**.
- d. Select **Backups**.

- e. Select **Restore configuration backup**.
- f. Select the backup file you want to restore, click **<OK>** or press Enter.
- g. Select **<Yes>** to continue.
- h. Enter the password used to encrypt the backup files.

The restoration process starts.

After the process finishes, the system restarts automatically.



Note: Your `SSH` connection will drop if the IP address of USM Appliance changes as a result of the restoration.

- i. Log in to display the AlienVault Setup menu again.
- j. Select **System Preferences**.
- k. Select **Reset AlienVault API Key**.

To find out more, see [Reset the AlienVault API Key](#).

11. Return to the AlienVault Setup main menu, select **Reboot Appliance**, click **<OK>** or press Enter.

Restore Software on a USM Appliance Hardware

Sometimes you may want to restore the software on a USM Appliance hardware appliance to its factory status. To do this,

- Burn the corresponding ISO image to a USB drive.

For instructions, see [Burn the USM Appliance ISO Image to a USB Drive](#).

- Change the boot sequence so that USM Appliance boots from the USB.

For instructions, see [Changing the Boot Sequence of a USM Appliance Hardware](#).

- Restore USM Appliance from the USB drive.

For instructions, see [Restore USM Appliance from a USB Drive](#).

Changing the Boot Sequence of a USM Appliance Hardware

By default, the USM Appliance hardware appliance boots from its hard disk. When trying to restore the software on a USM Appliance to its factory status, you need to configure USM Appliance to boot from the USB drive instead. This section provides instructions for performing this task.

Starting from version 5.4, AlienVault ships USM Appliance hardware built on Hewlett Packard Enterprise (HPE) ProLiant Gen9 Servers. All prior versions of USM Appliance hardware are built on Supermicro servers. Follow the instructions pertaining to the USM Appliance hardware you have.

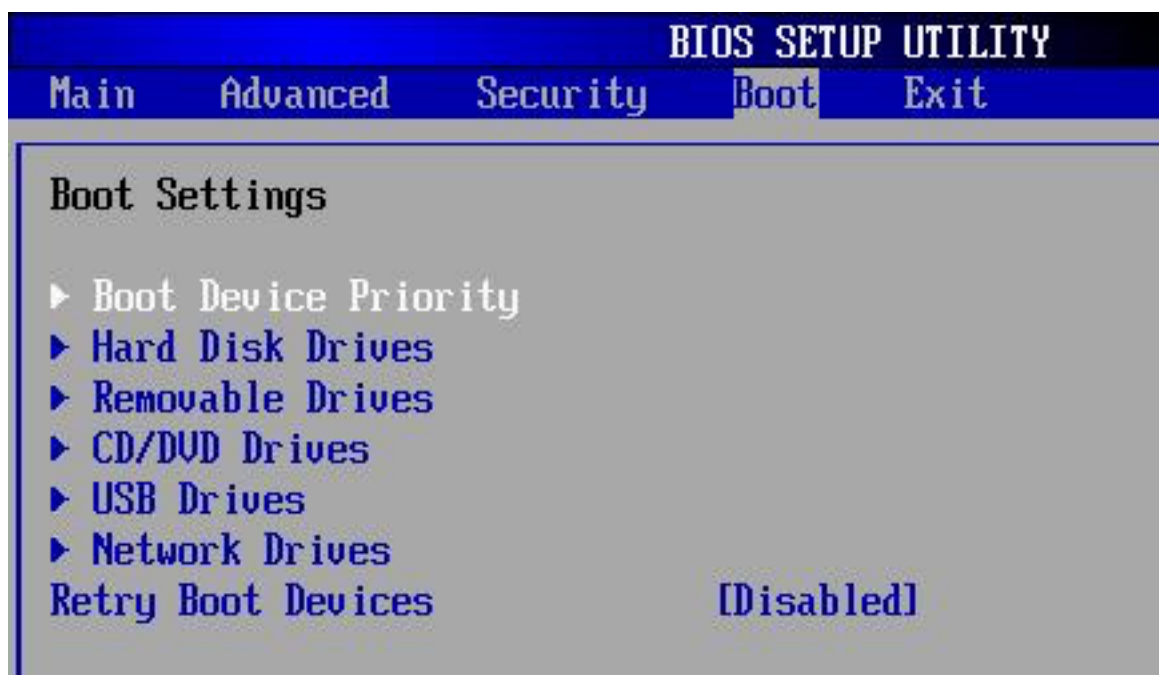
Changing the Boot Sequence on Supermicro Hardware

If the rear view of your USM Appliance hardware looks similar to the below, it is built on a Supermicro server.

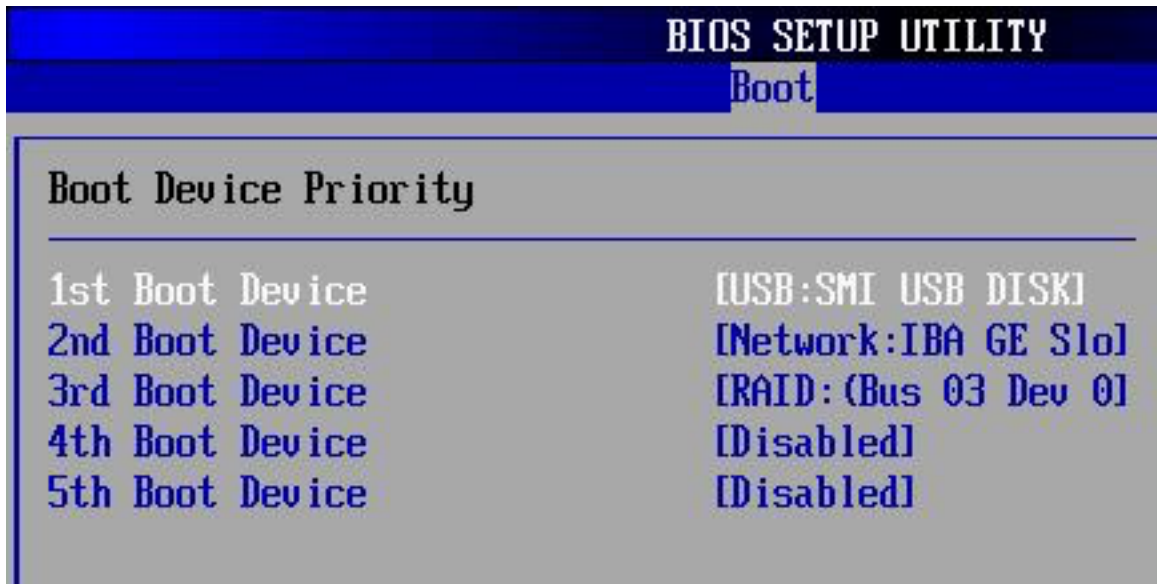


To configure a USM Appliance on Supermicro hardware to boot from a USB drive

1. Reboot USM Appliance, and press **Del** or **Delete** to launch the BIOS Setup Utility.
2. Using the arrow keys, move to **Boot**.



3. On Boot Settings, move the cursor to **Boot Device Priority** and press Enter.
4. On Boot Device Priority, move the cursor to **1st Boot Device** and select your USB device by using the + and – keys.



5. To exit, press **Esc**.
6. On Exit Options, move the cursor to **Save Changes and Exit** and press **Enter**.
7. Press **Enter** again to confirm.
8. Reboot USM Appliance.

Changing the Boot Sequence on HPE Hardware

If the rear view of your USM Appliance hardware looks similar to the below, it is built on an HPE ProLiant Server.

DL120 Gen9:



DL360 Gen10 with 1Gb interfaces:



DL360 Gen10 with 10Gb interfaces:



To configure a USM Appliance on HPE hardware to boot from a USB drive

1. Power on or restart USM Appliance.
2. Press the **F9** key, when prompted, to enter **System Utilities**.
3. Select **System Configuration** and then **BIOS/Platform Configuration (RBSU)**.
4. Select **Boot Options** and then **Legacy BIOS Boot Order**, press Enter.
5. Use the "+" or "-" key to move the USB entry to the top of the boot list.
6. Press **F10** to save your changes.
7. Restart the server.



Note: The USM Appliance Remote Sensor hardware is built on HPE ProLiant DL20 Gen9 Servers, but you can follow the same procedure above to change the boot sequence.

Restore USM Appliance from a USB Drive

Prerequisite

- Burn the corresponding ISO image to a USB drive.
- Change the boot sequence so that USM Appliance boots from the USB.



Warning: The process deletes all the data stored in your USM Appliance.

To restore USM Appliance from the USB drive

1. If not done already, insert the USB drive to your USM Appliance hardware appliance.
2. Reboot USM Appliance.
3. Select **Restore AlienVault <your-Appliance-Type>**.

Customers restoring to USM Appliance versions 5.2.3 and later see the following screen:

```
Found ocs_prerun* parameter in boot parameters...
The order to run: ocs_prerun
*****
Now run "ocs_prerun": mount --bind /lib/live/mount/medium/ /home/partimag...

WARNING!!!
If you continue, the DATA existing on the TARGET DEVICE will be DESTROYED. Be careful.
Are you sure you want to continue?
[y/N]
```

Customers restoring to USM Appliance versions up to 5.2.2 see screen below instead:


```
The jobs in /etc/ocs/ocs-live.d/ are finished. Start "ocs-sr -g auto restoredisk v4.3.1_h4.1_TrialPro_AllInOne6x1GB_2013-07-30-09-img sda" now.
Found ocs_prerun* parameter in boot parameters...
The order to run: ocs_prerun
*****
Now run "ocs_prerun": mount --bind /live/image/ /home/partimag...
mount: warning: /home/partimag seems to be mounted read-only.
Setting the TERM as linux
Starting /usr/sbin/ocs-sr at 2013-10-17 14:44:44 UTC...
*****
Clonezilla image dir: /home/partimag
*****
Shutting down the Logical Volume Manager
No volume groups found
Finished Shutting down the Logical Volume Manager
*****
Activating the partition info in /proc... done!
Getting /dev/sda1 info...
Getting /dev/sda2 info...
This program is not started by clonezilla server.
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/partimag/v4.3.1_h4.1_TrialPro_AllInOne6x1GB_2013-07-30-09-img" -> "sda (sda1)"
WARNING!!! WARNING!!! WARNING!!!
WARNING! THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL BE LOST:
*****
Machine: X8DTU-6+
sda (17976B_SMC2108_36003048003c4200019767123b169deb4)
sda1 (1.6T_ext3(In_SMC2108_)_36003048003c4200019767123b169deb4)
*****
Let me ask you again. Are you sure you want to continue? ?
[y/n] _
```


4. To continue, enter **y**.
5. Wait for the restoration process to complete.

```

Partclone v0.2.87 http://partclone.org
Starting to check image (-)
Calculating bitmap... Please wait... done!
File system:  EXTFS
Device size:    1.7 TB = 425302272 Blocks
Space in use:   36.6 GB = 8931455 Blocks
Free Space:     1.7 TB = 416370817 Blocks
Block size:    4096 Byte

Elapsed: 00:00:34 Remaining: 00:03:59   Rate:   8.02GB/min
Current Block: 11541533  Total Block: 425302272

Data Block Process:
 12.43%

Total Block Process:
 2.71%

```

6. After the restoration process finishes, disconnect your USB drive before the system reboots.

```

*****.
Running: ocs-tux-postprocess sda1
Trying to remove udev hardware record in the restored OS...
The specified destination device: sda1
Trying to remove udev persistent files. The devices to be searched: sda1...
Now searching possible device /dev/sda1...
done!
*****.
Running: ocs-update-syslinux -b sda1
Device /dev/sda1 is not a FAT partition.
Skip updating syslinux on that.
*****.
Running: ocs-install-grub -p "sda1" auto
Found grub partition: /dev/sda1
Found grub partition "/dev/sda1", which is on the restored partitions list (sda1). Will run grub-ins
tall later.
Found boot loader grub in the MBR of disk /dev/sda.
Found grub 2 installed in the restored OS.
Test if we can chroot the restored OS partition /dev/sda1...
Yes, we are able to chroot the restored OS partition /dev/sda1.
Trying to use the grub2 in the restored OS...
Running: run_grub2_from_restored_os "/dev/sda1" "/dev/sda1" "/dev/sda"
Re-installing grub2 on disk/partition /dev/sda with grub2 dir in partition /dev/sda1 and root partit
ion /dev/sda1...
Installing for i386-pc platform.
Installation finished. No error reported.
done!
*****.
End of restoreparts job for image MBX.
End of restoredisk job for image MBX.
*****
*****
Checking if udevd rules have to be restored...
This program is not started by Clonezilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...
Will reboot... 5 4 3 2 1 _

```



Note: If you forget to remove it, USM Appliance will boot from the USB drive again.

USM Appliance reboots and displays the initial login screen of the version you restore to.

7. Login as the `root` user using the system-generated password displayed on the screen.
8. Change the root user password as prompted.
9. Reboot the system again to finish the data restoration.

After the second reboot, the appliance is ready for you to use.

For other instructions regarding initial configurations, see [USM Appliance Initial Setup](#).

Update Your AlienVault License Key

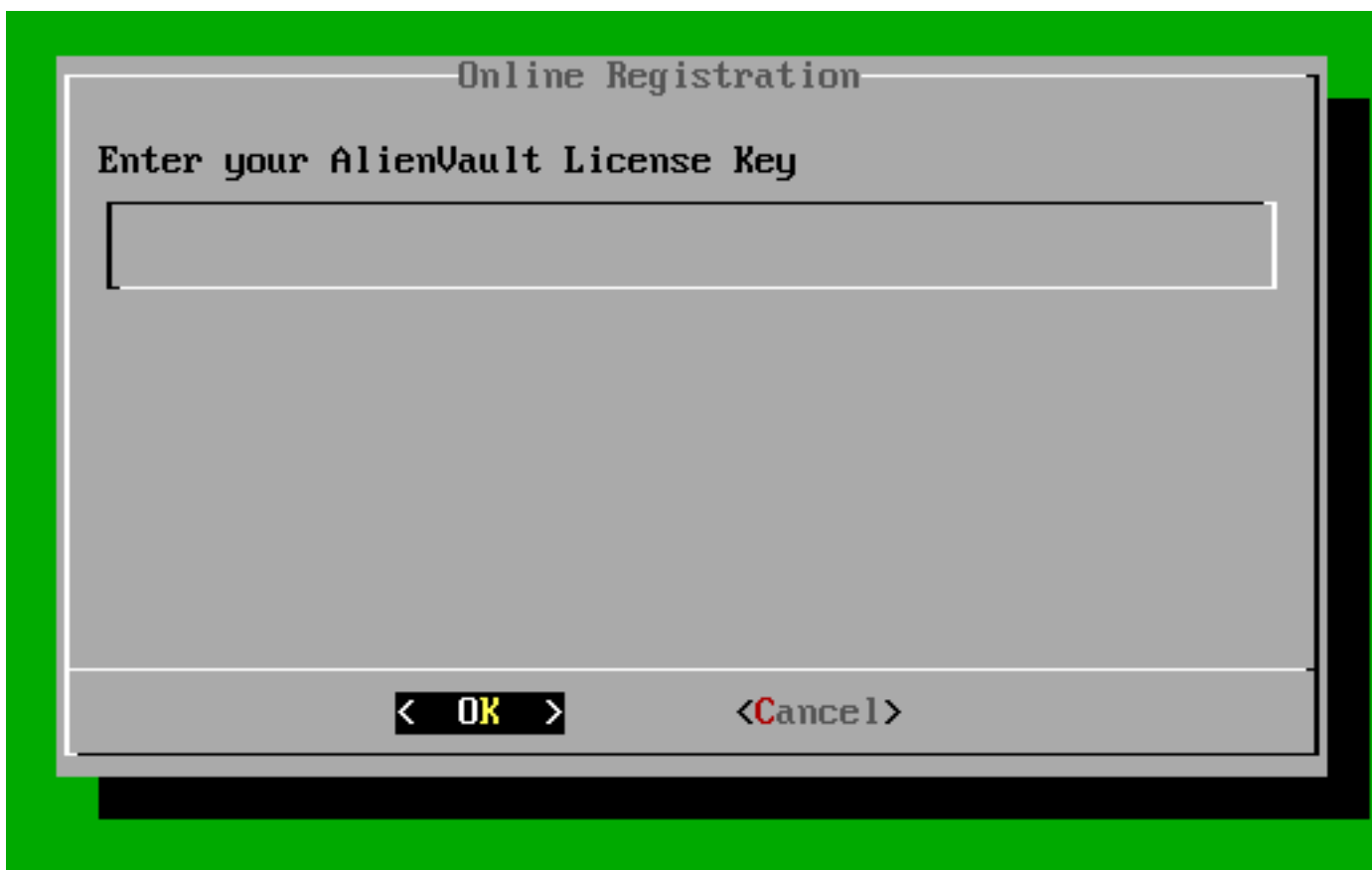
Occasionally, you may need to replace the AlienVault license key in your USM Appliance instance. For example, you may need to replace a trial license with a perpetual license, or you have migrated USM Appliance from VMware to Hyper-V, therefore you must use a different license key.

To replace the AlienApp license key in USM Appliance

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 **Update license information**.
4. Select **Online Registration** if you have Internet access. You will be prompted to enter the new license key:



5. Alternatively, if you do not have Internet access, select **Offline Registration**.



Important: To continue, you must have received a license file from AlienVault Support, see [Registering USM Appliance Offline](#) for more details.

6. Insert the USB drive containing the license file.
7. Click <**OK**> or press Enter to register the new license key.

The AlienVault License Key update process is now complete.

System Maintenance and Remote Support

AlienVault USM Appliance uses the Message Center to centralize all in-system errors, warnings, and messages. The Message Center also includes external messages sent by AlienVault about product releases and feed updates. You can only access the Message Center through the web UI.

The Remote Support feature in USM Appliance opens a secure, encrypted connection to the AlienVault Support Server through the web UI or the AlienVault Console. This allows the AlienVault Support staff to access, diagnose, and resolve any problems occurring in a USM Appliance component. Remote Support allows the AlienVault Support staff to work on solving the issues independently, after you have connected your USM Appliance components to the Support Server. All data exchanged with AlienVault Support is encrypted for security. The information exchanged is only available to AlienVault Support or the Engineering teams.

You should delete USM Appliance system logs and/or old event logs on a regular basis, otherwise the appliance may run out of space. Starting from version 5.2.1, USM Appliance adds a pre-check to its update script so that the update fails if the machine does not have enough disk space.

You may need to replace a power supply or hard disk drive on an AlienVault USM Appliance hardware should either one fail. These two components represent the most common cause of hardware failures, and can be replaced if necessary.

For more details, see the following topics.

Message Center	343
Remote Support	348
Locate the AlienVault License and System ID	352
Purge Old System Logs	353
Replace Disk Drives or Power Supplies	354

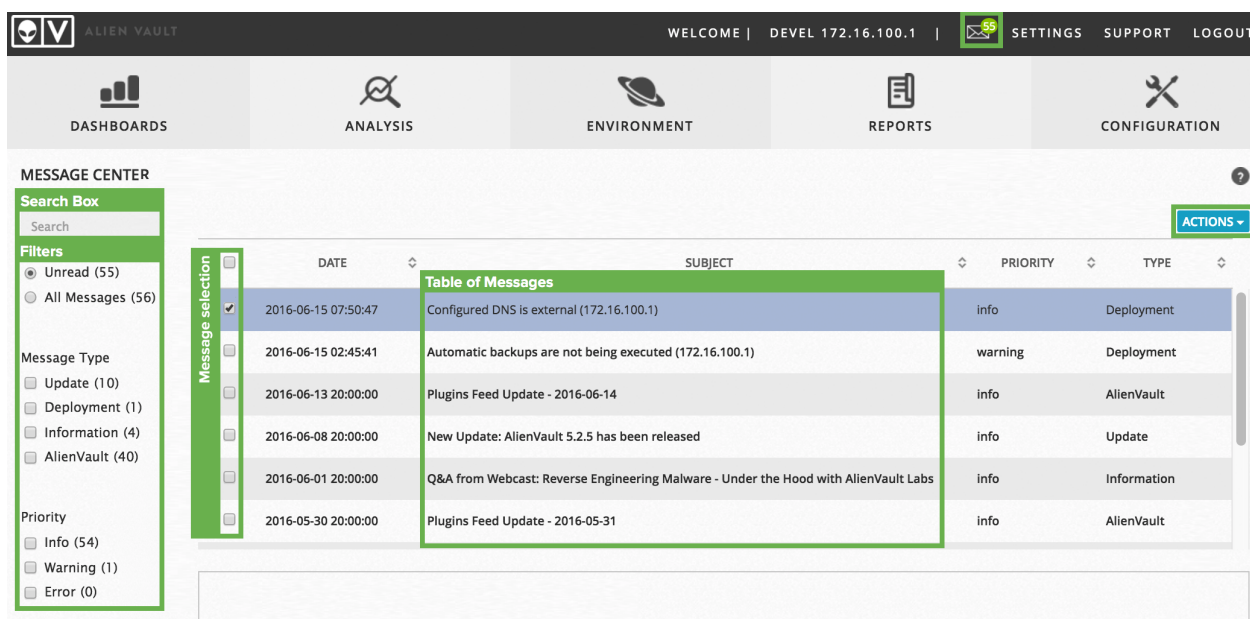
Message Center

AlienVault USM Appliance uses the Message Center to centralize all in-system errors, warnings, and messages. They also include external messages sent by AlienVault about product releases and feed updates. You can only access the Message Center through the web UI. All messages are displayed in the timezone configured for the user, but there are stored in the database as UTC (Universal Time Coordinated). You may see both displayed in some messages, as shown in the image below.

To view messages in the Message Center

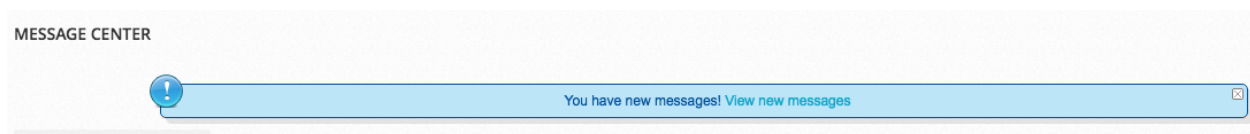
- Click the message icon () in the header menu.

The envelope icon shows the number of unread messages. If the number exceeds 99 messages, the icon displays 99+.



DATE	SUBJECT	PRIORITY	TYPE
2016-06-15 07:50:47	Configured DNS is external (172.16.100.1)	info	Deployment
2016-06-15 02:45:41	Automatic backups are not being executed (172.16.100.1)	warning	Deployment
2016-06-13 20:00:00	Plugins Feed Update - 2016-06-14	info	AlienVault
2016-06-08 20:00:00	New Update: AlienVault 5.2.5 has been released	info	Update
2016-06-01 20:00:00	Q&A from Webcast: Reverse Engineering Malware - Under the Hood with AlienVault Labs	info	Information
2016-05-30 20:00:00	Plugins Feed Update - 2016-05-31	info	AlienVault

If a new message arrives while you are on the Message Center page, USM Appliance displays an alert.



Message Types

These are the types of messages you might see in the Message Center.

Message types in the Message Center

Message Type	Description	Examples
AlienVault	Messages from AlienVault.	Plugins Feed Update - 2015-11-24
Deployment	System-generated messages regarding your USM Appliance instance.	Configured DNS is external (172.16.100.1)
Information	Miscellaneous messages regarding your USM Appliance instance.	Become an AlienVault Certified Security Engineer
Update	System-generated messages regarding updates.	New Update: AlienVault 5.2 has been released

Message Priorities

All messages are sorted by priority in the system.

Message priorities in the Message Center

Message Priority	Description	Examples
Info	These messages provide useful information to the user.	<ul style="list-style-type: none"> • AlienVaultCustomer Success Initiatives - Letter from the CEO. • Enable log management. • Plugin version out of date.
Warning	These messages specify that something in the environment has changed, and that USM Appliance is no longer functioning as it was configured. Warnings are also generated as precursors to Errors when USM Appliance detects a situation that could potentially disrupt normal operation if allowed to continue.	<ul style="list-style-type: none"> • Configuration backup could not be completed. • Log management disrupted. • Sensor connection lost.

Message priorities in the Message Center (Continued)

Message Priority	Description	Examples
Error	These messages concern something in USM Appliance that is no longer working or will stop working in a short period of time. These issues should be resolved as soon as possible to prevent service disruption.	<ul style="list-style-type: none"> Disk space is critically low. The remote system is not connected to the AlienVault API.

Search and Filter Messages

A search box in the upper left-hand corner of the Message Center lets you search all message content.

The screenshot shows the Message Center interface. At the top, there is a search box containing the word "plugins". Below the search box, there are several filter sections: "Unread (33)", "All Messages (34)", "Message Type" (with options for Update, Deployment, Information, and AlienVault), and "Priority" (with options for Info, Warning, and Error). The main area displays a list of messages with columns for DATE, SUBJECT, PRIORITY, and TYPE. A green box highlights the search box and the filter sections, with an arrow pointing to the search results. The search results show several messages, including "New Update: AlienVault 5.2.4 has been released" and "Plugins Feed Update - 2016-05-17".

The message filters that appear beneath the search box allow you to focus on a subset of messages. See table below for description on what each filter means.

Search filters in the Message Center

Filters	Description
Unread (n)	Use this filter to show messages that have not been read or all messages. The table of messages displays the unread messages in bold until the user clicks on them. The number between parentheses indicates the number of messages for each option.
All Messages (n)	
Message Type	<p>Use this filter to choose which message type to display. See Message Types for more information.</p> <p>The number next to each filter indicates the number of messages for each type. These numbers correspond to the first filter option that you choose. For example, if Unread is selected, and you choose Deployment under Message Type, the number in parentheses shows unread messages for Deployment.</p>
Priority	<p>Use this filter to choose which message priority to display. See Message Priorities for more information.</p> <p>The number next to each filter indicates the number of messages for each priority. These numbers correspond to the first filter option that you choose. For example, if All Messages is selected, and you choose Warning under Priority, the number in parentheses shows all warning messages.</p>



Note: You can select several filters at the same time by clicking the checkbox next to each filter. The table of messages displays the messages that match the checkbox(es) selected.

View a Message

Messages are displayed in a table format. By default, this table is sorted by date, from the newest to the oldest. All columns, except for the Actions column, can be sorted in ascending (▲) or descending (▼) order by clicking the (↔) icon. The triangle icon indicates which column is being sorted currently.

Each line in this table corresponds to a message.

Messages can come from the following sources

- External server — These messages are sent from AlienVault. Every hour the system checks if there are new messages. The server hosting the message is *messages.alienvault.com*, which uses port 443. The external server signs all messages and USM Appliance checks the signature to verify the authenticity.
- System status — These messages correspond to the operation of USM Appliance in real time. For this reason, they update frequently.

They consist of the following status types:

- Backup task in progress.
- One or more plugin configuration files have been deleted.
- Unable to analyze all network traffic.
- User Activity — These messages correspond to user activities within USM Appliance. For example, when a user executes a backup on **Configuration > Administration > Backups**, and the backup ends with an error, this will generate a message.

The screenshot shows the 'MESSAGE CENTER' interface. On the left, there's a sidebar with filters: 'Unread (49)', 'All Messages (54)', 'Message Type' (Update (9), Deployment (1), Information (4), AlienVault (40)), and 'Priority' (Info (54), Warning (0), Error (0)). The main area displays a table of messages with columns: DATE, SUBJECT, PRIORITY, and TYPE. The first message is highlighted in blue.

DATE	SUBJECT	PRIORITY	TYPE
2016-06-08 06:34:43	Configured DNS is external (172.16.100.1)	info	Deployment
2016-06-08 02:21:19	New Update: AlienVault 5.2.4 has been released	info	Update
2016-06-08 02:11:22	See What's New in OTX! New Version Now Available	info	AlienVault
2016-06-08 02:11:09	Plugins Feed Update - 2016-05-31	info	AlienVault
2016-06-08 01:35:12	Q&A from Webcast: Reverse Engineering Malware - Under the Hood with AlienVault Labs	info	Information
2016-05-16 20:00:00	Plugins Feed Update - 2016-05-17	info	AlienVault

Below the table, the details of the selected message are shown:

2016-06-08 06:34:43

The configured Domain Name Server is external to your environment. As a result, your asset names won't be discovered. At 2016-06-08 10:34:43 UTC.

- Configure an internal DNS:
 1. Go to *AlienVault console* (alienvault-setup)
 2. *System Preferences / Configure Network / Name Server DNS.*

To view the entire message

- Click the message line in the table.

The message details appear below the table, as shown in the previous illustration.

Delete a Message

In version 5.2 and earlier, only USM Appliance admin users can delete messages in Message Center. Starting from version 5.3, a normal user can delete a message after the admin user has granted him the **Message Center - > Delete Messages** permission in a template. For instructions on how to use a template, see [Configuring User Authorization with Templates](#).

To delete a message

- Select one or more messages and click **Actions > Delete**.

A confirmation message displays, asking you to confirm.



Important: Deleting a message deletes it from the system. There is no way to recover the message.

Remote Support

The Remote Support feature in USM Appliance opens a secure, encrypted connection to the AlienVault Support Server through the web UI or the AlienVault Console. This allows the AlienVault Support staff to access, diagnose, and resolve any problems occurring with a USM Appliance component. Remote Support allows the AlienVault Support staff to work on solving the issues independently, after you have connected your USM Appliance components to the Support Server.

All data exchanged with AlienVault Support is encrypted for security. The information exchanged is only available to AlienVault Support or the Engineering teams.

Typically, you open a ticket with AlienVault Support first and only establish a remote support connection upon their request. You can establish multiple sessions using the same ticket number for different USM Appliance components. But a support engineer may ask you to open a new ticket if it is an unrelated issue. During the remote support session you can communicate with the AlienVault Support team by phone or email at any time.

Prerequisites

To use Remote Support, you will need

- The ticket number you received from AlienVault Support.
- An Internet connection for the machine establishing the remote connection.
- A connection to TCP Ports 22 and 443 at `tractorbeam.alienvault.com` (50.16.174.234).

This connection allows for communication between the Support Server and the USM Appliance component being diagnosed. Your Domain Name System (DNS) must be able to resolve the IP address of `tractorbeam.alienvault.com` within 20 seconds, otherwise the connection will fail.



Important: Because `SSH` does not support a proxy configuration, you cannot use a proxy server for remote support.

Use Remote Support

You can establish the remote support connection either from the USM Appliance web UI or the [AlienVault Console](#).

To run remote support from the USM Appliance web UI

1. At the top menu, go to **Support > Support Tools > Remote Support**.
2. From the **Add Connection** list, select the component you want AlienVault Support to diagnose.
3. In the **Ticket Number** field, type the 8-digit ticket number.



Important: Be careful not to include any spaces before or after the ticket number.

4. Click **Connect**.

USM Appliance displays a status message indicating that it is in the process of establishing a tunnel.

SUPPORT ?

[HELP](#) [SUPPORT TOOLS](#) [DOWNLOADS](#)

DIAGNOSTIC TOOL | REMOTE SUPPORT

Connecting to Remote Support will open an encrypted connection for AlienVault Support to diagnose any issues with your AlienVault system(s). All data will be secure and available only to AlienVault Support. Audit logs detailing actions taken by the support representative will be made available upon request.

Add Connection
 VirtualUSMAInOneLite [192.1] ⌵
 Ticket Number
 00084246
 CONNECT

OPEN CONNECTIONS

COMPONENT	PORT REDIRECTION	ACTION
VirtualUSMAInOneLite [192.1]	connected	

SHOWING 0 TO 1 OF 1 COMPONENTS FIRST PREVIOUS NEXT LAST

Establishing tunnel, this may take a while....



Note: If the Support Server cannot validate the ticket number, USM Appliance displays an error message. If this occurs, contact AlienVault Support again.

After the Support Server establishes a connection, the Open Connections table displays the active connections to the components being diagnosed, and their respective ports.

SUPPORT ?

[HELP](#) [SUPPORT TOOLS](#) [DOWNLOADS](#)

DIAGNOSTIC TOOL | REMOTE SUPPORT

Successfully connected

Connecting to Remote Support will open an encrypted connection for AlienVault Support to diagnose any issues with your AlienVault system(s). All data will be secure and available only to AlienVault Support. Audit logs detailing actions taken by the support representative will be made available upon request.

Add Connection
 --Select a component-- ⌵
 Ticket Number

 CONNECT

OPEN CONNECTIONS

COMPONENT	PORT REDIRECTION	ACTION
VirtualUSMAInOneLite [192.168.73.159]	ssh:48229, https:48230	DISCONNECT

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

The Support Server also sends you an automated email that it has made a connection.

When AlienVault Support completes work on the issue, they communicate their results and update the ticket. You can request a log of all their activity at this point, or you can request it later by phone or email.

- After the troubleshooting session ends, click **Disconnect** next to the active connection you want to end.

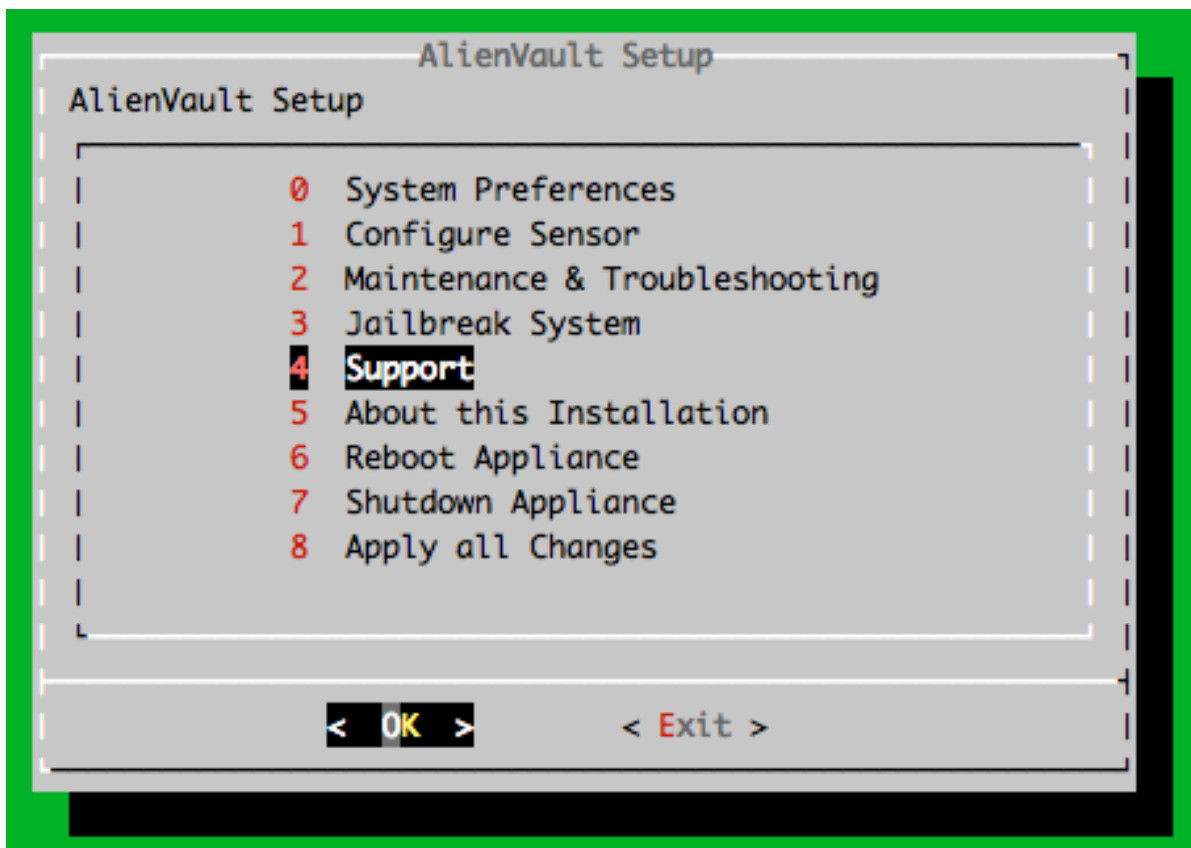
You should receive another automated email informing you that the connection has ended.

To run remote support from the AlienVault Console

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

The AlienVault Setup menu displays.

2. Select **Support** and click **OK**.



3. On the **Remote Support** screen, type the 8-digit ticket number, and click **OK**.



Important: Be careful not to include any spaces before or after the ticket number.

A black screen appears and your request begins processing. This may take several seconds.

When the connection is established with the Support Server, the following message appears:

```
Connected to AlienVault Support. Press [Enter] to continue.
```

You also receive an automated email that a connection has been made.

4. Press **Enter**.

The console returns you to the Support screen.

When AlienVault Support completes work on the issue, they communicate their results, and update the ticket. You can request a log of all their activity at this point, or you can request it later by phone or email.

5. To disconnect, from the Support screen, select **Remote Support**.

The Manage Connectivity information screen appears and prompts you with the following message:

```
Are you sure you want to disconnect from AlienVault Remote Support?
```

6. Click **Yes**.

The black screen reappears. After several seconds you receive a notification that the secure connection has disconnected.

```
Disconnected from AlienVault Remote Support.  
Press [Enter] to continue
```

You will also receive another automated email informing you that the connection has ended.

Locate the AlienVault License and System ID

When contacting AlienVault Technical Support, you are often asked to provide the AlienVault license or system ID of your USM Appliance so that we can verify the authenticity of the installation or reset the license if needed.

To find the license and system ID of your USM Appliance installation

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

The AlienVault Setup menu displays.

2. Select **About this Installation** and press Enter.

USM Appliance retrieves the system information

```
AlienVault Version: ALIENVAULT 5.4.3 (alienvault-vmware-aio-6x1gb)
Installation Date: Fri Dec 1 08:16:29 2017 (alienvault4 cd)
System ID: [REDACTED]
Profile: All In One
License:
    system_id: [REDACTED]
    key: [REDACTED]

Press [ENTER] to continue
```

- AlienVault Version denotes the USM Appliance version installed on the system. The name in the parentheses, `alienvault-vmware-aio-6x1gb`, provides details on the comparable hardware package, which in this case is the USM Appliance All-in-One with six 1GbE network interfaces.

Note: USM Appliance upgraded from version 4.8 or earlier may be missing some important hardware profile packages, causing issues for updating to later versions. For details, see our knowledge-base article: [Known Issue: AlienVault "profile" meta package is missing from units installed prior to version 4.9.](#)

- system_id is the unique identifier for this installation.
- key is the AlienVault license assigned to the installation when you [Register USM Appliance](#).

Purge Old System Logs

You should delete USM Appliance system logs and/or old event logs on a regular basis, otherwise the appliance may run out of space. Starting from version 5.2.1, USM Appliance adds a pre-check to its update-script so that the update fails if the machine does not have enough disk space.

To purge old system logs and/or clear system update caches

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 **Clear System Update Caches** to remove the local repository of the downloaded package files.
5. Alternatively, select **Purge Old System Logs** to remove the compressed (.gz) files in `/var/log`.
6. Press Enter after the process completes.

Replace Disk Drives or Power Supplies

You may need to replace a power supply or hard disk drive on an AlienVault USM Appliance hardware should either one fail. These two components represent the most common cause of hardware failures, and can be replaced if necessary.

AlienVault Support must confirm that your appliance needs a new disk drive or power supply before you can receive a replacement. Open a support ticket to report the issue and make your request.

See [AlienVault Technical Support](#) for information about opening a ticket.

Replace Disk Drives

If you need to replace a disk drive for an USM Appliance hardware, you can do it while the appliance is powered up.

You can determine if an appliance has a failed disk drive by checking for a red-colored LED on the front panel of the appliance or by using the RAID management software.

To replace a disk drive

1. Push in the red-colored switch on the carrier.



2. Use the black lever to pull the carrier out of the drive bay.



3. After you remove the disk drive from the carrier, you need to remove four screws.
There are two screws on each side of the carrier.



4. Confirm the replacement is the same size or larger than the failed drive.
5. Remove the defective disk drive from the tray.
6. Insert the new drive with the SATA connections facing the rear of the tray.



7. Make sure the screw holes are aligned before hand-tightening the screws.
8. Slide the drive into the bay and press the black lever to lock it.



Replace Power Supplies

If you need to replace a power supply for an USM Appliance hardware, you can do it while the appliance is powered up. The table below helps you determine the status of the power supplies.

700 Watt Power Supply LEDs

State	Indication
Solid green	System is on.
Solid amber	System is off and plugged in or 5V standby is on.
Blinking amber	Power supply internal temperature has reached 63 degrees Celsius. The power supply will shut down if the temperature reaches 70 degrees Celsius.

To identify a failed power supply

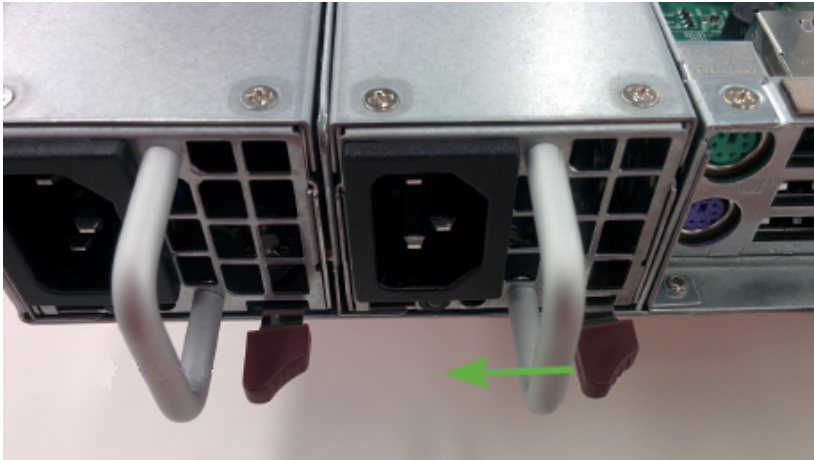
1. On the front panel of the appliance, look for the illuminated "i."



2. On the back of the appliance, check the power supplies for an amber-colored or unilluminated LED that indicates a power supply has failed.

**To replace a power supply**

1. After you identify the failed power supply, unplug its power cord.
2. Push the red-colored lever to the left and then pull the metal handle to release the power supply.

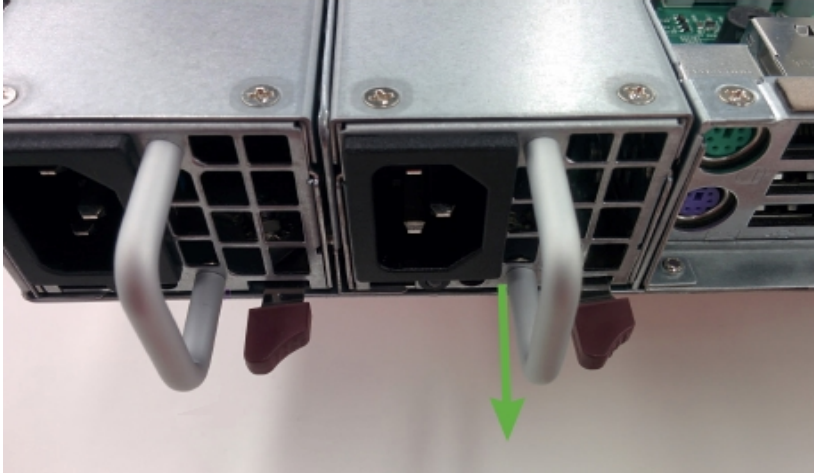


The power supply should release from the bay.

3. Insert the replacement power supply into the bay.



4. Confirm the power supply is locked in place by gently pulling on its metal handle.



5. Plug the power cord into the replacement power supply and make sure that the LEDs are green for both power supplies.

