AlienVault® Appliance Monitoring Service
Proactive, expert maintenance service of your USM Appliance™ assets

AlienVault® Appliance Monitoring Service (AMS) provides you with a proactive, expert service that accelerates and simplifies your ability to maintain the performance and security of your AlienVault USM Appliance™ assets. This remote service puts time back in your day by offloading essential but time-consuming regular maintenance of your AlienVault deployment.

The Appliance Monitoring Service enables you to focus on responding to threats and improving your security posture while AlienVault handles the essential maintenance of up to 15 AlienVault USM appliances (All-in-One, Sensor, Logger, Server) for one low price, including:

› Hourly check-ups of all your AlienVault devices (hardware appliances, virtual appliances, or cloud appliances) to ensure your appliance is running as effectively as possible

› Monthly updates managed by AlienVault Support

› Fast identification, diagnosis, and problem resolution

Most support programs are designed to be reactive — once an appliance stops working, the support team jumps on the problem. Our Appliance Monitoring Service is different — it ensures your AlienVault USM Appliance devices are healthy, fully functional and problem-free, providing continuity to your threat detection and response capabilities.

AlienVault AMS enables your IT team to focus on responding to alarms generated by the USM platform and monitoring compliance instead of spending time verifying system performance and installing updates.

How the Appliance Monitoring Service Works

The AlienVault AMS encrypts all communication between your systems and our server. We log all activity performed during the hourly automated checks and the monthly updates. We gather only the data that is relevant to health and usage of your USM deployment—the AMS does not have access to any other aspects of your environment.

The Appliance Monitoring Service includes both hourly health checks and monthly updates:

Hourly Health Checks

Every hour, the AlienVault AMS diagnostic tool will conduct an automated, detailed assessment of the health of your USM appliances to identify minor problems before they become major issues including:

› Ensuring your USM appliances have the latest Threat Intelligence updates installed

› Verifying the integrity of the USM Appliance packages installed on your system

› Checking all USM Appliance processes

› Confirming USM Appliance disk usage is within expected thresholds, as well as swap, connectivity, and database health

Monthly Updates

Every month, an AlienVault Certified Engineer (CE) will update your appliance to the latest AlienVault firmware version to ensure that your threat detection, response, and regulatory compliance capabilities are fully up to date. This monthly update includes:

› Ensuring that all AlienVault USM Appliance devices in your deployment are running the latest firmware, including ad-hoc updates and patches

› Verifying after the update that the update was successful and that the appliance is functioning correctly

› Deploying the update in a time window that minimizes disruption to security and network operations

Note: Appliance Monitoring Services are delivered remotely

What's not included in the Appliance Monitoring Service:

› The Appliance Monitoring Service does not include any type of security monitoring, vulnerability detection, intrusion detection or any type of security service. AlienVault CEs cannot provide any type of security assessment or opinion as to the security of a customer's network. If you are looking for a Managed Security Service Provider (MSSP), we can recommend an AlienVault Certified MSSP.

› The Appliance Monitoring Service does not include support for unsupported deployments, custom scripts, third-party software or other functionality that the customer or a third party has added.

› The Appliance Monitoring Service does not manage systems that have an improper installation or are not operated in accordance with AlienVault's Specifications or the Product Documentation.

## How the Appliance Monitoring Service differs from AlienVault Support and Maintenance

The Appliance Monitoring Service is separate from an AlienVault Support and Maintenance contract. AlienVault Technical Support provides the following functions, as part of our standard Support and Maintenance agreement:

› Analyzing challenges that prevent the product from operating as it was designed, and determining if the problem was a result of a Defect or Configuration Error

› Escalating and explaining discovered Defects to the Engineering Team and updating the Customers about the status of forthcoming patches

› Pointing Customers to general documentation related to your questions

› Providing basic instructions to properly configure the product when the customer is unaware of how to configure AlienVault USM to achieve a specific behavior

› Receiving and understanding the customer's product ideas and properly communicating the idea to the product management team

› Troubleshooting and validating hardware failures to recommend RMA process

› Identifying challenges that the customer is trying to solve and provide best practices to get the most benefit from the product

Detailed list of system checks delivered as part of the hourly health check:

The Appliance Monitoring Service performs the following steps, whether you have an All-in-One appliance or separate USM Appliance components:

USM SERVER	USM SENSOR	USM LOGGER
• Encrypt all data sent to our server • Evaluate Server logs to analyze disk usage, CPU usage and database usage, and take corrective action before critical situations arise • Identify last event processed to verify regular data collection • Verify that DB backups are running as expected and being cleared out • Monitor DB size and raw log size, to prevent uncontrolled growth • Check for any defunct processes and disk space • Identify dropped packets • Verify hardware profile packages • Log any issues as support tickets for resolution • Take corrective action as necessary to resolve the logged issues • Assign to support queue if issue cannot be resolved in two hours	• Encrypt all data sent to our server • Monitor DB size and raw log size, to prevent uncontrolled growth • Check for any defunct processes and disk space • Log any issues as support tickets for resolution • Take corrective action as necessary to resolve the logged issues • Assign to support queue if issue cannot be resolved in two hours	• Encrypt all data sent to our server • Check overall disk usage • Log any issues in Salesforce as support tickets for resolution • Take corrective action as necessary to resolve the logged issues • Assign to support queue if issue cannot be resolved in two hours
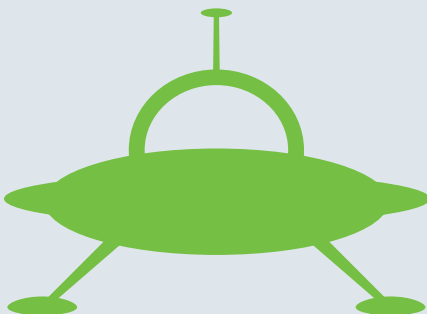
About AlienVault

AlienVault® has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and **award-winning approach**, **trusted by thousands** of customers, combines the essential security controls of our all-in-one platform, AlienVault® **Unified Security Management**™, with the power of AlienVault's **Open Threat Exchange**®, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource constrained IT teams.

For more information visit **www.AlienVault.com** or follow us on **Twitter (@AlienVault)**.