



Microsoft Advanced Threat Analytics

Licensing Datasheet

Behavioral analysis for advanced threat detection

Microsoft Advanced Threat Analytics is an on-premises software product designed to help you protect your enterprise from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity (user, devices, and resources) behavior.

The sophisticated analytics detect suspicious user activities, known malicious attacks and security issues, and reports results on a simple attack timeline.

Licensing Details

At general availability, you can purchase Advanced Threat Analytics (ATA) either standalone with a Client Management License (CML) – available per user or per Operating System Environment (OSE) – or through one of the following Microsoft license suites that provide multiple Microsoft products or cloud services at a significant discount over standalone license prices:

- Enterprise Client Access License (ECAL) Suite
- Enterprise Mobility Suite (EMS)
- Enterprise Cloud Suite (ECS)

A user CML permits the management of any OSE accessed by one user. An OSE CML permits management of one OSE accessed by any user.

ATA licenses are required only for client OSEs (or server OSEs used as client OSEs) that are on or accessed by end user devices authenticated by an Active Directory managed by Advanced Threat Analytics.

License Options		
	Per user	Per OSE/device
Through Enterprise CAL Suite per-user license	●	
Through Enterprise CAL Suite per-device license		●
Through Enterprise Mobility Suite user subscription license	●	
Through Enterprise Cloud Suite user subscription license	●	
Standalone license – Open L&SA estimated retail price, annualized*	USD \$80	USD \$61.5

** Pricing shown is an estimate only (L&SA = License + Software Assurance), and can vary by country. Please contact your Microsoft reseller or Microsoft representative for a quote.*

Microsoft Advanced Threat Analytics Licensing Datasheet

FAQ

Q. What is an Operating System Environment (OSE)?

A. An Operating System Environment (physical or virtual) is defined as all or part of an operating system instance which enables separate machine identity or separate administrative rights, and instances of applications configured to run on the operating system instance. A physical hardware system can have one physical OSE and/or one or more virtual OSEs.

Q. What does Advanced Threat Analytics monitor?

A. ATA inspects traffic to and from domain controllers (through port mirroring) and also monitors network traffic to analyze which users are accessing which resources from which devices. ATA can also be configured to collect data from your existing Security Information and Event Management (SIEM) or Syslog server.

Q. How many licenses do I have to buy to use ATA?

A. You must license as many users or OSEs as are being monitored by the ATA software. Licenses are only required for client OSEs (or server OSEs used as client OSEs) that are on or accessed by end user devices authenticated by an Active Directory that ATA is monitoring. Therefore the number of licenses you need will depend on:

- The domain controllers you configure ATA to monitor
- The users or user devices contained in the AD forests or domains that are managed by those domain controllers

Q. Why is licensing focused on the OSE, not the user?

A. By licensing all client OSEs (or server OSEs used as client OSEs) that are on or accessed by end user devices, a customer is effectively licensing all users that use those devices. Consequently, customers may find it simpler to license on a per-user basis.

Note that ATA acquired via the ECAL Suite per device license permits monitoring of any OSE on one device.

Q. Do I need to buy licenses for disabled or inactive users in the Active Directories that ATA is monitoring (e.g. user IDs of former employees that have been disabled, but may still be stored)?

A. No, there is no need to buy licenses for disabled accounts. The ATA product will still monitor all traffic, including any potential authentication attempts using a deactivated user ID, but we do not require you to purchase a license for them.

Q. I have a central SIEM system installed. Do I need to buy separate licenses to monitor SIEM or Syslog server events with ATA?

A. No. While can ATA collect and analyze relevant information from your SIEM or Syslog servers, a separate or additional license is not required to monitor this data source.

Q. Do I get Advanced Threat Analytics if I'm an existing ECAL Suite customer? Do I have to pay more for it?

A. If you have active Software Assurance on your ECAL Suite licenses through August 1 2015, then you will automatically receive rights to Advanced Threat Analytics, at no additional cost. Any mid-agreement true-ups will also include rights to Advanced Threat Analytics, at your existing agreement price.

Note: Prices for ECAL Suite per-user licenses are increasing after August 1 2015 (not due to ATA inclusion), but will not affect you if you have an active ECAL Suite purchase agreement as of this date. If you are signing a new agreement or renewing an agreement after August 1 2015, then you will receive a quote based on the new user license prices.

Q. Do I get ATA if I'm an existing EMS or ECS customer? Do I have to pay more for it?

A. Any EMS or ECS active subscription as of August 1 2015, will automatically receive rights to Advanced Threat Analytics, at no additional cost, until your subscription ends. Any mid-agreement true-ups will also include Advanced Threat Analytics, at your existing subscription price, until the end of the subscription term.

Note: Prices for EMS and ECS user subscription licenses are increasing after August 1, 2015 but will not affect you if you have an active subscription as of this date. If you are signing a new subscription or renewing a subscription after August 1 2015, then you will receive a quote based on the new prices. For EMS pricing, please review [Enterprise Mobility Suite pricing page](#).

Q. If my current license coverage for ECAL Suite, EMS, or ECS is only for a segment of my organization's employees, how do I get the use rights for ATA across the rest of my employees?

A. If you have users or devices in the Active Directories being monitored by ATA, but not covered by your existing ECAL, EMS, or ECS licenses, then you can purchase standalone ATA Client Management Licenses for those remaining users (with User CMLs) or user devices (with OSE CMLs).

Q. When Microsoft releases future versions for Advanced Threat Analytics, will I have to buy a new license or will I get free upgrades?

A. With EMS and ECS user subscription licenses, you get rights to the latest version of Advanced Threat Analytics at no additional cost, until your subscription ends. Mid-agreement true-ups will also include rights to the latest version of ATA, at your existing subscription agreement price, until the end of your subscription term.

For ECAL Suite and standalone ATA CMLs, our standard Software Assurance (SA) rules apply, where major version releases will require you to have active SA as of the date the new version is released. Note that service packs (bug fixes, patches) are made available to all customers, irrespective of SA coverage.

Q. How much does ATA cost?

A. Pricing varies by program, region, agreement type, and whether you are buying ATA standalone or as part of a Microsoft license suite such as the ECAL Suite. For example, ATA standalone license purchased via Microsoft Volume Licensing Open Program may have an Estimated Retail Price of USD \$160/two years for the User CML and USD \$123/two years for the OSE CML. Please contact your Microsoft reseller or representative for a price quote specific to you. Note that Microsoft does not determine pricing or payment terms for licenses acquired through resellers.

Q. How do I buy ATA?

A. ATA is currently sold via Microsoft's Volume Licensing programs, including Enterprise Agreement (EA), Open, MSDN, and Service Provider License Agreement (SPLA), among others. Please contact your Microsoft reseller or representative for a quote. Links to learn more about our VL programs or to contact sales can be found on the Advanced Threat Analytics website here: <http://www.microsoft.com/en-us/server-cloud/products/advanced-threat-analytics/default.aspx>.