Applied Satellite Technology Limited

AST INTEGRA See & Control Terms of Use

Including INTEGRA See, See+, Control Lite and Control

Enabling Global Connectivity

INTRODUCTION

These terms of use govern the relationship between Applied Satellite Technology Ltd and the Client.

DEFINITIONS

- AST INTEGRA See – Visibility of usage in Mbytes for each satellite service subscribed to, across 12 categories and shows the top 10 Applications and Protocols used at a given time in a billing month
- AST INTEGRA See+ – As INTEGRA See but enhanced with additional features including category expansion and full usage visibility
- AST INTEGRA Control Lite – As INTEGRA See+ but also provides blocking and automatic threshold alerting via e-mail at application level
- AST INTEGRA Control – Complete real-time visibility and alerting in Mbytes plus blocking and bandwidth shaping of categories and applications for each satellite service subscribed to.
- AST – Applied Satellite Technology Ltd
- Value Added Services – ASTs existing services within our INTEGRA suite
- Firewall – A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
- IP – Internet Protocol
- Web Security – A set of controls for web-based traffic
- AST Global Customer Services – ASTs 24/7/365 Global Customer Support
- Network Protocols – A protocol is a formal set of rules, conventions and data structure that governs how computers and other network devices exchange information over a network
- MyASTportal – ASTs airtime provisioning and management service/website
- VPN – Virtual Private Network
- CDR – Call Data Records
- ISDN – Integrated Services Digital Network
- Applications - A software program that you use via a PC/laptop, online or on mobile devices.
- Category – A section in AST INTEGRA Control and See that contains group of applications, usage and controls
- Handshake – The process by which two devices initiate communications

AST INTEGRA See & Control Terms of Use

NOTE: to aid readability, any references to ‘INTEGRA See and Control’, should be taken to mean the INTEGRA See and Control suite of services (including See, See+, Control Lite and Control).

1. AST INTEGRA See and Control work independently of ASTs existing value-added services which consist of firewall rules, web filtering and intrusion prevention. AST INTEGRA See and Control provide real time application visibility & control based on inspection of packets in an IP flow.

2. AST INTEGRA See and Control provide visibility of IP traffic plus the identification and control of applications over the satellite data service used. All data is inspected in real-time via the IP flow of traffic, identified as applications or protocols and are placed in 12 categories to allow blocking, alerting and bandwidth management. This is superior identification and blocking technology and allows greater granularity; however, this is based on best efforts as applications are constantly changing and evolving.

3. For ASTs application identification system to identify application traffic accurately, it will allow a small amount of traffic to pass to complete a handshake. Therefore, even with blocked applications or categories, you will still see a small amount of data on the AST INTEGRA See reports, which will be chargeable.

   a) If the handshake is initiated outside of the AST INTEGRA Network any usage that is then picked up will be classified as an existing or unmanaged session – this will show in network protocols

   b) Example: a file download started at home or outside of the AST INTEGRA Network that is continued once connected in the AST INTEGRA Network - the data usage will be an existing or unmanaged session. This is application dependant.

   c) If usage gets blocked in the AST INTEGRA Network and then unblocked, there may not be another handshake. Therefore, AST INTEGRA may not be able to classify the data correctly.

   d) Example: user blocks peer to peer, upon unblocking the data usage may be classified as an existing or unmanaged session. This is application dependant.

e) If AST INTEGRA Control is unable to identify traffic, it may classify the data as unmanaged flow or existing session. AST INTEGRA Control has a setting that stops this type of traffic after 120 seconds, this will enable AST INTEGRA Control the chance to reclassify the data. For advanced users, there is the ability to decide whether they would like the data to stop after 120 seconds or whether it should continue to flow. Unmanaged flow or existing sessions fall into the Network Protocols category, meaning that the category or data cannot be blocked. By default, AST INTEGRA Control is set to stop unmanaged flows and existing sessions after 120 seconds.

4. The AST INTEGRA Network operates a Web Security engine that allows AST to block various URL/Web sites, with gambling, pornography, advertisements and software updates being blocked by default. Please note these services are ‘best effort’ as these sites and services are continuously changing and evolving.

    a. Should you wish to allow software updates then please ensure these are not blocked in AST INTEGRA Control and contact AST Global Customer Services who will remove the default blocking policy from the web security “engine”.

5. Mobile to Mobile - data cannot be view/monitored or controlled via INTEGRA See or Control. Some basic IP controls are possible for Inmarsat L-band and Iridium Certus IP data and services. This will still be monitored using standard monitoring/suspension tools in My AST Portal.

6. VPN traffic may be detected however the applications used within the VPN session cannot be identified.

7. All data usage values used in the AST INTEGRA Control or the AST INTEGRA See system are measured using IP data. CDR usage is measured in the mobile network by the satellite providers. Converting the data to IP results in a larger figure. Therefore, information from the AST INTEGRA See and Control system cannot be used to dispute billing information based on CDRs.

8. If no data is visible in AST INTEGRA See but usage is known to have taken place, please contact your AST Account Manager.

9. Subscribe/un-subscribe to service – Applied immediately. Charging applies pro-rata for the first month, monthly in-advance and full month on deactivation.

10. AST INTEGRA Control measures 1Megabyte as 1000bytes. 1000 bytes has been selected as satellite network operators use different variations and combinations of 1000 and 1024 bytes.

    a. By using 1000bytes for 1MB and 1000Mbyte = 1GB, AST ensures calculations based on usage result in the largest possible number, so that you are even more protected from utilising more data or bandwidth than you desire.

11. All monitoring is based on calendar month.

12. Non-IP data, Voice and ISDN services do not pass through AST INTEGRA. These services plus $spend monitoring will need to continue to be monitored against standard CDRs via My AST Portal.

13. Streaming IP is included in AST INTEGRA and will have the same rules applied as selected for Background/standard IP. Steaming IP usage is not included in the counting/controlling/alerting functionality as this is billed by time.

14. Once subscribed to one of the AST INTEGRA services, if your package allowance is IP background data this will become your default monthly threshold. For all other allowances, these will be set to a default amount of 600Mbytes (50 per category) this should be reviewed and amended to accommodate your requirements.

15. When Subscribing to AST INTEGRA Control or Control Lite this will remove any existing carrier-based MB alerting (Inmarsat services only).

16. When unsubscribing to AST INTEGRA Control or Control Lite, if monitoring/alerting of carrier-based MB is required this will need to be applied in the Monitoring/Reporting area of MY AST Portal.

17. AST INTEGRA suite – There is no pricing of usage in AST INTEGRA Control as it is based on IP data usage. Billing CDRs are priced.

18. My AST Portal data traffic is whitelisted and therefore use is not counted and is always accessible from the terminal regardless of AST INTEGRA Control

settings. A small amount of data will be consumed for this action.

19. Network protocol category cannot be blocked as this will affect the operation of your device. Bandwidth Management can still be applied but should be used with care and only applied by a user with detailed IP data knowledge.

20. If the Bandwidth Management has been configured incorrectly it can result in a degraded service experience. It is possible to reset back to the default settings as they were at the time of subscribing to AST INTEGRA Control.

21. Category blocking – 3 levels of blocking

    a) All – Blocks all categories including Network Protocols but not My AST Portal.

    b) Categories – Blocks at category level.

    c) Applications – Block applications.

22. Category Bandwidth Management – 2 levels

    a) All – when setting the bandwidth at ALL this will be the maximum bandwidth available to share amongst all categories below.

    b) Category – by setting the bandwidth at Category level this will set the maximum available to be shared by all applications within the category.

    c) To preserve the quality of your service AST INTEGRA actively limits Peer to Peer to 50% of your bandwidth when other applications are in use.

23. Application Signature database

    a) New applications and changes to current applications happen frequently. To keep up to date with these changes AST will update its systems at least monthly. These updates may include additional applications that can now be detected, changes to how an application is identified, as well as changes to the classification of applications.

    b) Some applications are simple to recognise whereas others are very complex and change frequently.

    c) Some applications may have dependencies on other applications, which may not be within the same application category. An example of this is Facebook Messenger (within the Real-Time Communication) which is dependent on Facebook (within Social Networking) to allow the user to authenticate. Therefore, blocking the Social Networking category would affect the usability of an application within the Real-Time Communication category (Facebook Messenger). However, blocking Real-Time Communication would not restrict the usage of the Facebook application.

All of this (a,b,c above) means is that it is possible for applications to be misclassified.

If you believe you have identified such an issue, please report this to AST Global Customer Services.

24. AST INTEGRA See and Control can identify encrypted applications with a high degree of accuracy, and although it can identify the application, it does not have visibility of the content. However, it is not able to identify application usage within VPN tunnels.

25. AST will continue to allow firewall rules/web filtering, if a block is applied at either AST INTEGRA Control or firewall/web level the block will be applied. AST INTEGRA Control may be required to work alongside traditional firewall rules to meet a customer's requirements. Both AST INTEGRA Control and firewall rules will be used in conjunction, and anything restricted via either method will be restricted. One method will not override another.

26. The services are provided as part of a complex network solution, on an 'on-demand' basis and are subject to the availability of capacity on the applicable network. Services may be temporarily unavailable or limited because of capacity limitations, network equipment failures, distress or any other emergency pre-emption as required by AST or a supplier or may be temporarily interrupted or curtailed due to modifications, upgrades, repairs or similar activities of the supplier. AST has no liability for unavailability or malfunction of provider networks.

27. AST may vary the technical specification of services from time to time if AST provides the customer with prior written notification of such variation.

Disclaimer

To the best of our knowledge, the information contained herein is accurate and reliable as of the date of publication; however, we do not assume any liability whatsoever for the accuracy and completeness of the above information.

Applied Satellite Technology Ltd makes no warranties which extend beyond the description contained herein.

Any information given in this statement does not constitute any warranty of merchantability or fitness for a particular use. It is the customers' responsibility to inspect and to test our products in order to satisfy themselves as to the suitability of the products to their particular purpose.

The customers are responsible for the appropriate, safe and legal use, processing and handling of our products. The information contained herein relates to our materials when not used in conjunction with any third-party materials. Applied Satellite Technology Ltd will not accept any liability with respect to the use of its products in conjunction with other materials. Without derogating from the above, the standards and the analysis methods (if an analysis method is mentioned above) which the above statement refers to, are only those which are expressly mentioned in the above statement and no other standards and/or analysis method should be implied in any way from the above information. This certificate will not derogate in any way from the limitation of liability under the contract between the customer and our company.