INTEGRA See & Control Terms of Use

INTRODUCTION

These terms of use govern the relationship between DSD E.U.R.L. and the Client.

DEFINITIONS

- INTEGRA See – Provides visibility of usage in Mbytes for each satellite service subscribed across 12 categories and shows the top 10 Applications and Protocols used at a given time in a billing month

- INTEGRA Control – Provides visibility and alerting in Mbytes plus blocking and bandwidth shaping of categories and applications for each satellite service subscribed per month

- DSD – DSD E.U.R.L.

- Value Added Services – DSD's existing services contained in our INTEGRA Network

- 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 – Cyber security and Intrusion prevention

- DSD Global Customer Services

- 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

- MY Portal – DSD's 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 online or on mobile devices.

- Category – A section in INTEGRA Control and See that contains Applications usage and controls

- Handshake

INTEGRA See & Control Terms of Use

1. INTEGRA See and Control works independently of DSD's existing value added services which consist of firewall rules, web filtering and intrusion prevention. INTEGRA See and Control provide real time application control based on inspection of packets in the IP flow.

2. 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.

3. The INTEGRA Network operates a Web Security engine that allows DSD 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.

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

5. In order for DSD`s application identification system to identify application traffic accurately it will may to allow a small amount of traffic to pass to complete handshake. Therefore even with blocked applications, or categories, you will still see a small amount of data on the INTEGRA See reports which will be chargeable.

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

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

DSD, Bâtiment A – 71/73 rue Desnouettes 75015 PARIS - France - Tél. : +33 183645916
Fax : +33 183646333 N° TVA : FR 25418473104 - Siret : 418 473 104 000 36 - APE : 4652Z - dsd@dsd.fr

V. 7 Mar 2019

c) If a usage gets blocked within the INTEGRA Network and then unblocked there will not be another handshake, therefore 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 existing or unmanaged session. This is application dependant.

e) If INTEGRA Control is unable to identify traffic, it may classify the data as unmanaged flow or existing session. INTEGRA Control has a setting that stops the traffic after 120 seconds, this will enable 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, INTEGRA Control is set to stop unmanaged flows and existing sessions after 120 seconds.

6. Mobile to Mobile - data is not inspected and therefore cannot be view/monitored or controlled. This will still be monitored using standard monitoring/suspension tools in My Portal

7. VPN may be detected however if it is initiated behind the terminal the applications cannot be identified

8. All data usage values used in the INTEGRA Control or the INTEGRA See system is 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 INTEGRA See and Control system cannot be used to dispute billing information based on CDRs.

9. If no data is visible in INTEGRA See please contact your DSD Account Manager.

10. Subscribe/un-subscribe – Applied straight away. Charging applies prorate for the first month, monthly in-advance and full month on deactivation

11. 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.

12. By using 1000bytes for 1MB and 1000Mbyte = 1GB, DSD 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.

13. All monitoring is based on calendar month

14. Non IP data, Voice and ISDN services do not pass through INTEGRA. These services plus $spend monitoring will need to continue to be monitored against standard CDR's via My Portal.

15. Streaming IP is included in INTEGRA and will have the same rules applied as selected for Background IP, Steaming IP is not included in the counting/controlling/alerting functionality.

16. Once subscribed to INTEGRA Control 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 600 (50 per category) this should be review and amended to accommodate your requirements.

17. When Subscribing to INTEGRA Control this will remove any existing carrier based MB alerting. (existing customer only)

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

19. INTEGRA Control – There is no pricing of usage in INTEGRA Control as it is based on data IP usage. Billing CDR's are priced.

20. My Portal is whitelisted and therefore is always accessible from the terminal regardless of INTEGRA Control settings. A small amount of data will be consumed for this action.

21. Network protocol category cannot be blocked as a standalone category as this will affect the operation of your device. Bandwidth Management can still be applied.

22. If the Bandwidth Management has been configured incorrectly, it is possible to reset back to the default settings as they were at the time of subscribing to INTEGRA Control.

23. Category blocking – 3 levels of blocking

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

   b) Categories – Blocks at category level

   c) Applications – Block applications

24. Category Band Width Management – 2 levels (available after training session)

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

25. Application Signature database

   a) New applications, and changes to current applications happen frequently. To keep up to date with these changes DSD 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. So 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.

   d) All of this means is that it is possible for applications to be mis-classified.

   e) If you believe you have identified such an issue please report this to DSD Global Customer Services in the normal manner.

26. INTEGRA See\Control can identify most encrypted applications with a high degree of accuracy, although we can identify the application we cannot access the content. However it is not able identify application usage within VPN tunnels.

27. DSD will continue to allow firewall rules/web filtering, if a block is applied at either INTEGRA Control or firewall/web level the block will be applied. INTEGRA Control may be required to work alongside traditional firewall rules to meet a customer's requirements. Both 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.

28. 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 DSD or a supplier or may be temporarily interrupted or curtailed due to modifications, upgrades, repairs or similar activities of supplier. DSD has no liability for unavailability or malfunction of provider networks.

29. DSD may vary the technical specification of services from time to time provided that DSD 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.

DSD E.U.R.L. 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. DSD E.U.R.L. 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.

DSD, Bâtiment A – 71/73 rue Desnouettes 75015 PARIS - France - Tél. : +33 183645916
Fax : +33 183646333 N° TVA : FR 25418473104 - Siret : 418 473 104 000 36 - APE : 4652Z - dsd@dsd.fr

V. 7 Mar 2019