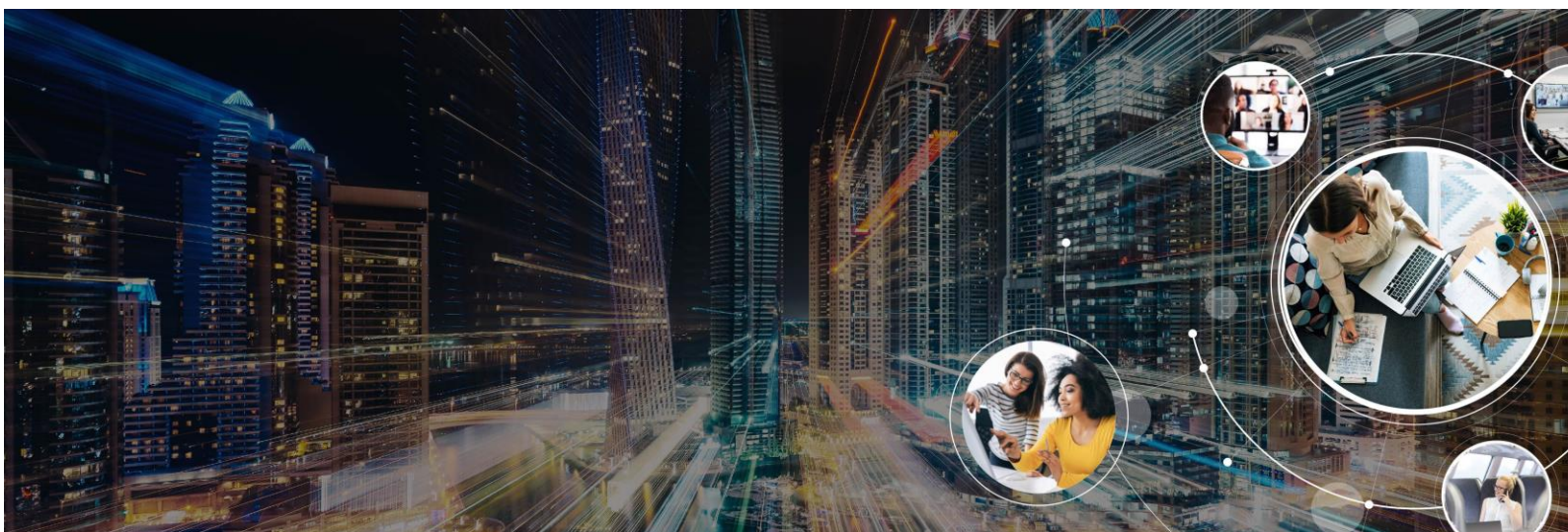




Charterhouse Voice & Data Ltd

Fusion Teams Telephony SIP and Call Plans Service Description

Contents

<i>Contents</i>	2
<i>1. Introduction</i>	6
<i>2. Service Overview</i>	6
<i>3. Service Features</i>	8
3.1. Calling Line Presentation (CLIP)	8
<i>Rejection</i>	9
3.2. Calling Line Restriction (CLIR)	10
3.3. Call Park, Transfer & Conferencing	11
3.4. Emergency Call Divert	11
3.5. Fraud Alert	12
3.6. CLI Flexibility	12
3.7. Call Admission Control	13
3.8. Call Barring	14
3.9. Fax and DTMF support	14
3.10. Emergency, Non-Emergency and other short code Calls	15
3.11. Gamma SIP Trunks for Hosted Partners	16
Calling Line Data Requirements for Gamma SIP Trunks for Hosted Partners	17
Number Format	18
UK Domestic and Non-Domestic SIP Trunks	18
Diversion Header	18
Call Screening	19
<i>4. Service Characteristics</i>	20
4.1. Endpoints	20

<i>Endpoint Naming</i>	20
4.2. Calling Plans and Number Formats	21
<i>Presentation CLI (A-Number)</i>	21
<i>Network CLI (A-Number)</i>	22
<i>B-Numbers</i>	22
<i>Number Portability</i>	23
4.3. Maximum Calls per Second (CPS)	23
4.4. Channel bandwidth.....	23
4.6. IP Addressing and DNS	24
4.7. Codecs.....	24
4.8. Session Failover and Endpoint Resilience.....	25
<i>Destination unreachable</i>	25
<i>SIP Response Codes</i>	25
<i>Prevention of Session loss</i>	25
4.9. Customer Premises Equipment.....	26
4.10. Network Security	26
<i>5. Customer Network Design Options</i>	26
5.1. Single Site	27
5.2. Enhanced build.....	28
<i>Call Admission Control (CAC)</i>	28
<i>Fail over and resiliency</i>	28
5.3. Active Standby	29
<i>Call Admission Control (CAC)</i>	29
<i>Fail over and resiliency</i>	30
5.3.1 Resilience+	31

<i>Call Admission Control (CAC)</i>	32
<i>Fail over and resiliency</i>	32
5.4. Load Share	33
<i>Call Admission Control (CAC)</i>	33
<i>Fail over and resiliency</i>	34
5.5. Failover examples	35
<i>Scenario 1</i>	35
<i>Scenario 2</i>	35
<i>Scenario 3</i>	36
6. Network Access and Connectivity Options	36
6.1. Public Internet	36
<i>Access Control – Configuration of NonGamma access routers</i>	36
6.2. Private Interconnect	37
<i>Network Demarcation</i>	38
<i>Quality of service</i>	38
<i>Resilient Connectivity</i>	39
<i>Connection Types</i>	39
<i>IP Addressing and Gamma Ethernet connectivity</i>	39
7. Protocol & Signalling support	39
7.1. RFC Support	39
7.2. Signalling and Encoding	41
<i>Format of the SIP INVITE Field</i>	41
<i>Example of the initial SIP INVITE</i>	42
<i>Supported SIP methods</i>	43

<i>Supported SIP Responses</i>	<i>44</i>
7.4. Hunt-able SIP Responses	46
<i>8. Fraud Management Service description</i>	<i>48</i>
8.1 Functionality Overview	2
8.4 Status Information	3
8.5 Terms and Conditions.....	3
<i>New IPDC order</i>	<i>4</i>
<i>Daily Spend Limit.....</i>	<i>4</i>
<i>Weekly Spend Limit</i>	<i>4</i>
<i>Access/Edit Fraud Management for an existing Endpoint.....</i>	<i>4</i>
8.7 Partner Notification of Limit Breach	5
<i>End User Notification</i>	<i>7</i>
<i>Resetting after Breach.....</i>	<i>7</i>
9. Dialler Policy	7
10. Provisioning	7
11. Fault Handling, Escalation, and Reporting.....	7
12. Billing.....	8
13. Calls Between the Emergency Handling Centre and Emergency Authority	8
<i>Glossary</i>	<i>8</i>

SIP Service Description

1. Introduction

This document provides the technical specification of the Gamma SIP Trunk Service.

This document is written for Network Engineers, System Administrators, Field Engineers, and Technical Consultants who have been tasked with setting up, managing, troubleshooting the Gamma SIP Trunk Service. This guide assumes that those who use it will have a basic knowledge of VoIP services & protocols.

The document should be read in conjunction with the following documents related to the Gamma SIP Trunk Service:

- Gamma SIP Trunk Service Description
- Gamma SIP Trunk Service Billing Specification

To ensure that you are viewing the most up to date document, please refer to the Technical Support area of Gamma SIP Trunk Service documentation, which can be found on the Gamma Academy.

2. Service Overview

Internet Protocol Direct Connect (IPDC) is one the products forming Gamma's SIP Trunk Service, marketed and sold within the UK via authorised Channel Partners. The service provides VoIP connectivity for certified PBX's, allowing inbound and outbound telephony through Gamma's network for termination with both national and international destinations.

Gamma's SIP Trunking service uses SIP (Session Initiation Protocol) as the signalling method and offers both Public and Private Access to the service depending on the specific customer needs.

Please note – This Technical Specification relates to the core Gamma SIP Trunk Service and excludes the IP access to the Gamma network (whether supplied by Gamma or not) and any Customer Premises Equipment (CPE)

The Gamma SIP Trunking Service includes the following:

- CLIP (Calling Line Identity Presentation);
- CLIR (Calling Line Identity Restriction);
- Call Park, Transfer & Conferencing
- Emergency Call Divert
- Fraud Alert
- CLI presentation flexibility
- Call Admission Control
- Call barring
- Fax and DTMF support

The features listed above are supported in the Gamma network. However, it should be noted that the features are not guaranteed to be supported on every CPE platform connected to the Gamma SIP Trunk Service because of vendor interoperability issues.

The Gamma SIP Trunk Service provides SIP signalling as a method for Communication Providers to inter-connect with Gamma's VoIP network supporting calls to/from the PSTN as well as VoIP to VoIP calling between SIP accounts created within the Gamma SIP Trunk Service. The following types of calls will be supported across this interface:

- Voice calls to/from PSTN or geographic destinations (01,02)
- Voice calls to/from non-geographical, corporate or VoIP numbers (03, 05, 08)
- Voice calls to/from Premium numbers UK (09) and International
- Voice calls to/from Mobile destinations (07)
- Voice calls to/from International destinations (00..)

Operator, Emergency and non-Emergency calls (100, 101,111,112, 116xxx, 118, 119, 123, 159, 1800x, 195, 999).

Several number formats are supported for both DDI's and CLI's however, not all number formats are supported, for example, TEL URIs using the parameter "phone-context" are not supported and calls utilising such formats may experience issues including loss of service. Details of supported formats appear later in this document.

Gamma Channel Partners can access the Gamma SIP Trunk Service via public internet or private interconnects. These connectivity options include the following:

- Gamma provided Private and Public connections, Gamma IP Assured or Ethernet for example
- Public internet via third party Internet Service Providers (ISPs)
- Private Interconnect – Public IP Addressing – Layer 3 routing
- Private Interconnect – Private IP Addressing – Layer 2 VLAN

Gamma offers three design options as standard, for the configuration of the customer's Gamma SIP Trunk Service.

- A single site working off a single Gamma SBC HA cluster.
- Dual sites in active / standby mode working off different Gamma SBC HA clusters. Dual sites in load-balanced
- mode working off different Gamma SBC HA clusters.

The Gamma network will only respond to messages from equipment where the IP address is defined within the order process.

3. Service Features

Gamma support Network Number CLI presentation and Privacy definitions in accordance to RFCs 3323 and 3325, using P-Asserted ID and Privacy Headers only. We require customers to supply the PAID and, where required, the Privacy Headers, Gamma do not support the use of the invalid statute Remote Party ID (RPID) definitions and such Headers will be removed.

3.1. Calling Line Presentation (CLIP)

Calling Line Identification Presentation (CLIP) is a service that transmits a caller's number to the called party's telephone equipment during the ringing signal.

If the CPE connected to the Gamma network presents a geographic number in the UK National format, the Gamma Network will pass these details as the A-Number CLI into the PSTN or Mobile network. This outbound presentation will be supported by default if the number presented is as follows:

- A number in the UK national format without a leading zero presented by the Customer Premises equipment (CPE) as the A-number.
- A Gamma provided Geographic Number that is allocated to the Endpoint at order creation
- A Gamma provided Geographic Number that is allocated to the Endpoint at a later date via a Customer Change Request
- A Geographic number that is ported from another Carrier to the Gamma Network

The A-number is checked against a database on the Gamma network of geographic numbers that are allocated to the Gamma SIP Trunk Service Endpoint.

If the number presented does not meet the above criteria, the A-Number CLI presented will be a

default CLI, which by default is the first number in the Gamma allocated Geographic DDI range. This default CLI can be changed and set via the Gamma Portal.

If the presented number meets these criteria, the A-Number CLI is presented to the called party and the CLI information is presented in the Gamma Daily and monthly CDRs.

Gamma cannot guarantee consistent presentation of intended CLIs for calls made to mobile carriers as successful presentation of the intended CLI is entirely dependent on the mobile carriers use of these numbers and specific call flow. Mobile missed calls and voicemail notifications can often use the default CLI – the underlying network CLI (PAID CLI) – which is the customer selected default number or the first number in the Gamma allocated account range, rather than the intended CLI for presentation. Gamma were aware that calls to mobile carriers cannot guarantee consistent presentation of the intended CLI as successful presentation is entirely dependent on the carriers' use of these numbers and specific call flow. For instance, missed calls and voicemail notifications will often use the underlying network number rather than the intended CLI as the presented number.

We have been liaising with both Network Providers and have the following updates.

Both O2 and EE have performed upgrades on their network to resolve these issues. We have confirmed the problem has now been resolved following further testing in conjunction with both Network Providers. Should you experience any issues related to CLI Presentation, please raise a fault in the usual manner

For example:

Headers contained within Invite towards SIP Trunking Endpoint

From: <sip:+441625827748@83.245.6.117>;tag=3541226335-339769

Contact: [sip:+441625827748@83.245.6.117](tel:441625827748)

P-Asserted-Identity: [sip:+441625827748@83.245.6.117](tel:441625827748)

NOTE: With CLIP no modifications are performed for SIP Trunking untrusted requirements.

Rejection

You must ensure that any of your Gamma SIP Trunks where we have provided you with additional permissions around CLI presentation and flexibility, are configured to present a correctly formatted and valid CLI. Failure to do so will result in the end user experiencing call failures given we and other Communications Providers will block these call attempts at network level.

Please note, the Ofcom General Conditions are non-negotiable, and all traffic over the Gamma network must comply.

06 May 2024

https://www.ofcom.org.uk/__data/assets/pdf_file/0021/112692/Consolidated-General-Conditions.pdf

https://www.ofcom.org.uk/__data/assets/pdf_file/0021/116670/cli-guidance.pdf

The logic will be applied as follows:

1. Check all FROM/ PAID/ Diversion header user parts.
2. If From header contains anonymous or unavailable then skip further checks on FROMheader.
3. Check the user part is a properly formatted number i.e. leading + and set of repeating numeric characters (Gamma supports 10 digits, leading zero or E.164 format).
4. If we have a correctly formatted UK number check it is a valid length.
5. If we have a correctly formatted International number check it is a valid length.
6. Check if the FROM / PAID / Diversion header is not using an unallocated/spare International country code.

If steps 3, 4, 5 or 6 fail the call will be rejected on the Gamma network or in point 6, on the onward carrier network. This response is non configurable.

* Please note, calls to short-codes and emergency services are unaffected by this change.

** SIP trunk endpoints with CLI Flexibility will follow the CLI verification rules prior to the above logic being applied.

3.2. Calling Line Restriction (CLIR)

When the calling (A-Party) has requested privacy (CLIR), Gamma will enforce privacy in accordance with RFC3325 and recent UK standards. Calling party information, including From, Contact, PAsserted-Identity and associated Privacy Header (PAID) are withheld from an endpoint but it is a Channel Partners responsibility to ensure this occurs by implementing the definitions below.

For calls from the Channel Partner (CP) to Gamma, the CP must indicate that CLI is to be withheld by supplying the following mechanisms:

The FROM header CLI is used to indicate that the client is requesting privacy, <sip: [anonymous@anonymous.invalid](#)> is the only accepted Gamma method

If the CP provides a PAID Header, then there must be a Privacy Header containing the value "id" to prevent this number from being presented at the destination.

Privacy settings have been enabled on the portal appropriately.

For calls from Gamma to the Channel Partner CPE:

If the Privacy Header contains the value "id" then the PAID and Privacy Header (RFC 3325) are both removed from the outbound INVITE to the SIP Trunking endpoint. To provide true CLI restriction the caller must define that the FROM Header contains a CLI of <sip:

anonymous@anonymous.invalid>. It is the caller's responsibility to ensure they provide the appropriate Header definitions to provide true CLI restriction, CPs and Gamma are not responsible for anonymising the contents of the FROM Header.

Example:

Public Side Invite; (Going out to SIP Trunking Endpoint)

From: Anonymous <sip:anonymous@anonymous.invalid>;tag=3541226365-699915

Contact: <sip:anonymous@83.245.6.117:5060>

NOTE: No PAID Header is provided for anonymous inbound calls. It is removed to provide the calling party full anonymity.

3.3. Call Park, Transfer & Conferencing

The Gamma SIP Trunk Service provides the features listed below in the majority of cases but are not guaranteed on every platform connected to SIP Trunking because of vendor interoperability issues:

- Call Parking
- Call Transfer
- Conferencing

These features are supported via the SIP re-invite mechanism

3.4. Emergency Call Divert

The Gamma SIP Trunk Service provides the facility to pre-configure call diverts for both individual numbers and DDI number ranges from the portal. Under failure conditions, the user can logon to the portal and activate either all pre-configured numbers with a single action, or activate individual diverts as necessary. Once activated, these diverts become effective. Confirmation that these diverts are being enabled is provided via email to the registered user.

Deactivation is performed in the same manner as activation, again with email notification confirming successful deactivation.

The diverted destinations are subject to the same call barring option as the main SIP trunk, e.g. if the user does not allow calls to mobiles, then the divert destination options will also exclude mobile numbers.

The user will be billed for the diverted leg for all diverted calls.

Gamma does not support emergency diverts to international or other numbers which exceed 11 digits in length.

Users are constrained to a total maximum of 150 emergency call diverts configured per endpoint at any point in time.

Please note that the emergency diverts are enable within the Gamma core network. The range of standard SIP Trunking endpoint features (e.g. fraud alerts, CLI flexibility, call admission control) do not apply to CLIs with emergency diverts enabled.

3.5. Fraud Alert

Gamma SIP Trunk Service Endpoints are potentially vulnerable to fraudulent spend, particularly if the customer adopts weak access security to their PBX. The fraud alert function is a cost option that allows partners to set pre-arranged spend limits on individual SIP trunks.

These spend limits can be set to monitor both 24hr and 7 day periods with individual figures associated with both. On reaching 85% of the maximum spend in any period, an email and SMS alert will be sent to the partner. If the spend reaches 100% of the agreed limit a further email and SMS will be sent to the partner and all subsequent calls from that end-point will be barred.

Service can be restored by the partner logging onto the portal and resetting (or increasing) the spend count.

Please Note:

Calls to the emergency services 999, 112 & 18000 will be unaffected.

Inbound Calls are not affected.

Calls set-up via the emergency Divert function are excluded in the fraud calculation.

3.6. CLI Flexibility

As an optional service, Channel Partners can enable the ability to present NON Gamma Registered CLIs as the Presentation A-Number CLI.

The service supports the presentation of the following A-Number CLI types:

National Significant (1NNNNNNNNN, 2NNNNNNNNN, 3NNNNNNNNN, 7NNNNNNNNN, 8NNNNNNNNN) for UK numbers.

National Significant with leading zero (01NNNNNNNNN, 02NNNNNNNNN, 03NNNNNNNNN, 07NNNNNNNNN, 08NNNNNNNNN) for UK numbers.

E.164 (441NNNNNNNNN, 442NNNNNNNNN, 443NNNNNNNNN, 447NNNNNNNNN, 448NNNNNNNNN) for UK numbers.

SIP E.164 – with leading plus – (+441NNNNNNNNN, +442NNNNNNNNN, +443NNNNNNNNN, +447NNNNNNNNN, +448NNNNNNNNN) for UK numbers.

UK International (00441NNNNNNNNNN, 00442NNNNNNNNNN, 00443NNNNNNNNNN, 00447NNNNNNNNNN, 00448NNNNNNNNNN) for UK numbers.

SIP E.164 – with leading plus – (+CCNNNNNNNNNN) for non-UK numbers.

UK International (00CCNNNNNNNNNN) for non-UK numbers.

The presentation of any other A-Number CLI types, badly formatted CLI A-Numbers or UK revenue sharing numbers (9NNNNNNNNNN, 09NNNNNNNNNN, 449NNNNNNNNNN, +449NNNNNNNNNN and 00449NNNNNNNNNN) is not supported by Gamma and such numbers will be replaced by the default CLI, which is the first number in the Gamma allocated DDI range. The presentation number must not be a number that connects to a revenue sharing number which will generate excessive or unexpected call charges; the use of such numbers may result in Gamma suspending and/or withdrawing the use of the Presentation CLI Flexible Service

Presentation of Mobile A-Number CLI types (7NNNNNNNNNN, 07NNNNNNNNNN, 447NNNNNNNNNN, +447NNNNNNNNNN and 00447NNNNNNNNNN) excludes Personal numbers.

For calls made to the Emergency, Non-emergency & Operator Services (100, 101,111,112,116, 118,123,1800 and 999), only Gamma A-Number CLIs are accepted and must be in the National Significant (with or without a leading zero) or the SIP E.164 – with leading plus – format, any other A-Number CLI or A-Number CLI format will be overwritten by the default CLI, which is the first number in the Gamma allocated DDI range.

All A-Number CLIs will be “normalised” within the Gamma network to the SIP E.164 format for external presentation but Gamma are not responsible for subsequent carriers changing the presented A-Number CLI or its format.

CLI digit lengths are not policed, Channel Partners are responsible for this function.

Gamma will populate field 16 (“DDI”) of the Gamma SIP Trunking Daily/Monthly CDRs with the Presentation A-Number CLI presented in the SIP FROM Header field.

Gamma cannot guarantee the terminating carrier will display the Presentation A-Number CLI. For example, US carriers may display the P Asserted Identity (PAID) rather than the Presentation ANumber.

Some countries may block calls that originate outside the country with a presentation number for the country.

Gamma SIP Trunks for Hosted Partners provides additional capability for Presentation A-Number and PAID numbers. Please see section 3.11 for more information.

3.7. Call Admission Control

Through a process known as Call Admission Control (CAC), the maximum call limit of an endpoint defines its capacity for routing calls in the network. SIP Trunking customers pay a fixed monthly charge for the number of concurrent calls (channels) allowed on

their endpoint. As each customer endpoint will have 2 ports, one for outgoing and one for incoming the CAC limit will be allocated to both ports to allow maximum flexibility. Thus Gamma will support any combination of incoming or outgoing calls provided the total number of calls does not exceed the total channel allocation (i.e. CAC limit).

Maximum Total Calls – specifies the overall number of calls the endpoint will support, both ingress and egress.

Maximum Ingress Calls – specifies the maximum calls that may be placed from that endpoint to the Gamma network.

Maximum Egress Calls – specifies the maximum number of calls that may be placed to that endpoint by Gamma.

For example, if the channel limits is 100 concurrent calls, and there are 70 ingress calls, the maximum no of egress calls allowed will be 30.

In the case that the call control constraints are exceeded at a SBC, the invites will be rejected with either a SIP Response 486 or 503 depending on build type (See section 5).

Please note that SBC clusters configured prior to 2018 may respond with a 503 on channel exhaustion regardless of build type, this behaviour has been amended on all clusters configured from 2018 onwards as per the network policy.

3.8. Call Barring

By default, calls to international and premium numbers will be barred. Customers are able to modify their profiles to allow or restrict access to:

- International Numbers.
- Mobile Number
- Premium rate numbers (i.e. 09....).

Similarly, customers can modify their barring profile to allow or restrict all outbound and/or inbound calls. Calls to the emergency services 999, 112 remain unaffected irrespective of the barring applied.

3.9. Fax and DTMF support

The Gamma SIP Trunk Service will support Fax and Modem transmission subject to the following constraints:

FAX and Modem transport in band using G.711 a-law codec is supported.

Renegotiation to T.38 is supported. (subject to interoperability testing)

The use of G729 for in-band faxes is not supported as its compressed nature may cause tones and messages to be lost.

If the fax option for an endpoint is set to T.38 enabled then:

The Gamma network will attempt to re-negotiate [re-INVITE] to T.38 for fax calls for ingress (Customer to Gamma) calls on detection of a fax tone.

The Gamma network will accept a re-negotiation [re-INVITE] to T.38 for fax calls for egress (Gamma to Customer) calls.

The re-negotiation must be done using the re-INVITE mechanism after answer.

Due to different vendor implementations Gamma cannot guarantee T.38 interoperability with all vendors and will not accept responsibility if T.38 interoperability cannot be achieved with a specific vendors' implementation.

If the fax option for an endpoint is set to T.38 disabled, then:

All fax calls will be handled as G.711 pass through providing the customer has a G.711 codec available in his media profile.

If calls are made to another CP that does not support the method of transport for the tones, Gamma will not perform any form of inter-working between the two different methods.

The following methods will be supported to transport DTMF tones:

The Gamma core network will support the generation of 'In-band' or 'RFC2833' DTMF transport based on end-to-end negotiation.

RFC2833 is the preferred method for the transport of DTMF tones. Support of RFC 2833 is dependent on successful codec negotiation and requires the payload type 101 to be assigned. RFC2833 will be used with both G.711 and G.729 codecs.

In band over G.711 codec only

If a G729 codec is being used then DTMF tones should not be sent in-band, Gamma will not guarantee the delivery of in-band DTMF over a G729 codec.

3.10. Emergency, Non-Emergency and other short code Calls

Important Note: Gamma provide a VoIP service as defined by Ofcom, this can be used to support Emergency Services calls. Once the service is fully operational, 999/112 public emergency call services can be accessed and will be routed to one of a number of national emergency call handling agents. This emergency call handling agent may not be geographically the closest to the area code indicated by the calling CLI. The CLI presented will always be the site CLI, indicated as a VoIP service type from Gamma, so that the emergency services operator will check the address details on the National Database. It is the Operators responsibility to ensure that the address associated with the default site CLI is always up to date. Gamma provide Operators the tools to maintain these addresses.

Gamma and Ofcom expect that any calls originating on the Gamma network to emergency services will be presented with a CLI relating to the SIP service.

As a VoIP service SIP Trunking may not be possible, in the following circumstances:

- During a service outage where the end-customer loses connectivity for example, owing to a power outage or the failure of DSL routing equipment
- If an end-customer's account has been suspended

In such circumstances the end-customer should use their PSTN line to make the emergency call. In addition, the end-user should also be made aware that the emergency personnel would need to confirm the identity and the actual location of the caller when they dial 999/112.

Channel Partners should always clearly inform end-users of the above service limitations related to the Emergency Services support in line with the Ofcom Code of Practice related to VoIP Services. The SIP trunking service supports routing the following dialled short codes:

- 999 (Access to the Emergency services)
- 100 (Access to Operator Assistance)
- 101 (The national single non-emergency number for the Police Force)
- 111 (The national single non-emergency number for the NHS)
- 112 (Access to the Emergency services)
- 116 xxx (Harmonised Services of Social value)
- 118 (UK Directory enquiries)
- 123 (Access to Speaking Clock)
- 18000* to *18009 (Access to Voice Text Services for the Deaf)
- 195 (Access to Blind & Disabled Directory Enquiry Facilities)

3.11. Gamma SIP Trunks for Hosted Partners

Gamma SIP Trunks for Hosted Partners is another product in the SIP Service family. A variation of Gamma SIP, it is designed specifically for connection to hosted service providers. Customers are required to contract to additional regulatory conditions. This includes the responsibility to provide address and calling line information for the National Emergency Services database as described in section 3.10. Emergency, Non-Emergency and other short code Calls.

Customers provisioning a Gamma SIP Trunk for Hosted Partners must select one of the following options:

- UK Domestic: SIP Trunk is used for traffic originating in the UK
- UK Non-Domestic: SIP Trunk is used for traffic originating outside the UK

Configurations include the automatic provisioning of the standard SIP Trunking features:

- CAC for five calls per second inbound calls (from the customer) call rate.
- DTMF support for G.711 a-law pass-through and/or RFC 2833 (using data type 101 only)

Configurations include the automatic provisioning and control of the standard SIP Trunking features:

- ITU G.711 a-law and/or ITU G.729 codec support Call barring of :
 - - International calls
 - Premium number calls
 - Mobile number calls

- Fax support for G.711 a-law pass-through and/or T.38
- Fraud alerting
- Configuration support for :
 - Single site designs
 - Active-Standby redundant site designs
 - Load-Share redundant site designs

Calling Line Data Requirements for Gamma SIP Trunks for Hosted Partners

[Ofcom Guidance](#) on the provision of Calling Line Identification facilities and other related services requires Communications Providers to present a “valid, dialable telephone number which uniquely identifies the caller”. It is the responsibility of the partner using the Gamma SIP Trunk for Hosted Partners to ensure Calling Line data provided in calls sent to the Gamma network complies with Ofcom guidance.

The Gamma network will check the following SIP headers on calls from Gamma SIP Trunks for Hosted Partners to ensure the contents meet the Ofcom guidelines for valid, dialable numbers

06 May 2024

- From
- PAID (P-Asserted-ID)
- Diversion (if present)

Number Format

As defined by the [UK National Interconnect Council \(NICC\) Standard](#) ND 1439 the Gamma network requires the contents of From, PAID and Diversion headers to be E.164 with leading + format.

For example: sip: <+441632123456@domain;user=phone>

UK Domestic and Non-Domestic SIP Trunks

Gamma requires traffic to be separated into either a UK Domestic or UK Non-Domestic SIP Trunk based upon the PAID number. Calls with a PAID number in UK E.164 format (+44) must use a UK Domestic SIP Trunk. Calls with PAID number in E.164 format other than the UK (+non-UK country code) must use a UK Non-Domestic SIP Trunk.

Diversion Header

UK Domestic SIP Trunk for Hosted Partners

Diverted UK originated calls can be indicated by either or both of:

- Diversion header with the identity of the diverting party
- PAID header overwritten with the identity of the diverting party

In both cases, the diverting party CLI must be a UK number.

UK Non-Domestic SIP Trunk for Hosted Partners

The Gamma network will remove the Diversion header on incoming calls from a UK Non-Domestic SIP Trunk.

Call Screening

The Gamma network will apply the following rules to Calling Line data, depending on the type of SIP trunk for Hosted Partners.

The primary difference between the UK Domestic and UK Non-Domestic SIP trunk is the country of the number contained within the PAID field.

Calls with a non-UK PAID number using a UK Domestic SIP Trunk will be blocked.

Calls with a UK mobile PAID number(+447) using a UK Non-Domestic SIP Trunk are permitted however calls with a non-mobile UK PAID number using a UK Non-Domestic SIP Trunk will be blocked.

In addition to the PAID field, the format of numbers in the From and Diversion field (if present) are also checked.

SIP Trunk for Hosted Partner type	SIP Header Contents and Format	From	PAID	PAID if Diversion header present / Diversion
UK Domestic	"anonymous"	supported	blocked	blocked / blocked
	"unavailable"	blocked	blocked	blocked / blocked
	Premium (+449)	blocked	blocked	blocked / blocked
	UK Mobile E.164 leading plus (+447)	supported	supported	supported / supported
	UK E.164 leading plus (+44)	supported	supported	supported / supported
	INTL E.164 leading plus (+)	supported	blocked	supported / blocked
	Non-E.164 leading plus (no leading +)	blocked	blocked	blocked / blocked
	Other	blocked	blocked	blocked / blocked
UK Non-Domestic	"anonymous"	supported	blocked	Not supported
	"unavailable"	blocked	blocked	blocked
	Premium (+449)	blocked	blocked	Not supported
	UK Mobile E.164 leading plus (+447)	supported	supported	Not supported

	UK E.164 leading plus (+44)	supported	blocked*	Not supported
	INTL E.164 leading plus (+)	supported	supported	Not supported
	Non-E.164 leading plus (no leading +)	blocked	blocked	Not supported
	Other	blocked	blocked	Not supported

* the detailed implementation of regulatory requirements for this case is beyond the scope of this document. Please contact Gamma if you require more information.

Blocked calls will have a 603 Decline SIP message response.

Emergency Calls

There are no restrictions on emergency calls (999, 112, 18000)

4. Service Characteristics

4.1. Endpoints

An endpoint represents the unique IP address used by the Channel Partner's (CP) on-site signalling proxy for Customer Premises Equipment (CPE). This CP signalling proxy supports SIP protocol, transferring VoIP calls to and from the CP site. Each SIP Trunking customer will have one or more endpoints configured on the Gamma SBC. CPE equipment may connect via a single endpoint or multiple endpoints for added resilience.

Endpoint Naming

The following naming convention is used for identifying endpoints on the Gamma network:

Unique Endpoint Name + suffix e.g. DC2NYYABC1234_L1

The Unique Endpoint Name (DC2NYYABC1234) is an identifier to the Gamma SIP Trunk Service and helps ensure all IP interconnects are easily identified for reporting and fault resolution purposes.

Resilient endpoints can be easily identified by virtue of the fact that the naming convention has been extended to append an 'A' (Active), 'S' (Standby), 'L' (Load Share) or "R" (Resilience+) to the endpoint name. There will typically be 2 endpoints per design though may be more for larger Load share deployments

The Suffix differentiates the endpoint design type i.e.

_L1: A Loadshare endpoint

_A1: An Active endpoint in an Active/Standby design

_S1: A Standby endpoint in an Active/Standby design

_R1: A Resilience+ endpoint

The suffix will simply increment in the case of multiple loadshare or standby endpoints associated with the same design.

4.2. Calling Plans and Number Formats

Two calling plans are allocated to each Endpoint: one for incoming calls from the customer to Gamma (ingress), and one for outgoing calls from Gamma to the customer (egress). It is a requirement of the SIP Trunking product that the calling party (A-number) be validated to confirm the format and ensure that the number is owned by Gamma, so that the emergency services have an accurate record of the calling customer.

Customers are responsible for supplying both A-Numbers and B-Numbers in a valid format and not containing alpha characters, spaces, hyphens, full stops, etc.

Presentation CLI (A-Number)

A-numbers (SIP FROM, P-Asserted-ID) should be presented in E.164 format, i.e. +441611234567. The A-number is validated by the SBC and if it is not in the Gamma range it is overwritten with an agreed network CLI from the customer's Gamma-allocated range. It is a requirement of the SIP Trunking service that the calling party (A-number) be validated to confirm the format and ensure that the number is owned by Gamma, so that the emergency services have an accurate record of the calling customer.

If the CPE connected to the Gamma network presents a geographic number, the Gamma Network will pass these details as the A-Number CLI into the PSTN or Mobile networks. This outbound presentation will be supported by default if the number presented is as follows:

A-numbers are presented by the Customer Premises Equipment (CPE) in the SIP FROM and PAsserted-ID fields as E.164 format

It is a Gamma provided Geographic Number that is allocated to the Endpoint at order creation

A Gamma provided Geographic Number that is allocated to the Endpoint at a later date via a

Customer Change Request

A Geographic number that is ported from another Carrier to the Gamma Network

If the presented number meets these criteria the A-Number CLI will be sent to the PSTN/next hop network. The delivery of the Presentation Number is dependent on the terminating network and is not under the control of Gamma. This CLI information will be presented in the Gamma Daily and monthly CDRs.

The A-number is checked against a database on the Gamma network of geographic numbers that are allocated to the SIP Trunking Endpoint.

If the number presented does not meet the above criteria, the A-Number CLI that will be presented will be a default CLI, which is the first number in the Gamma-allocated Geographic DDI range.

For ingress calls, A-numbers are sent to customers as received by Gamma from other network operators.

Network CLI (A-Number)

Every endpoint must have at least one CLI from the Gamma-allocated range i.e. a non-ported in number. This default number is known as the Network CLI and will be presented in the case of emergency calls and other call scenarios where the presented is invalid. Physical address information must be associated with a network CLI and it is the customer responsibility to ensure this address information remains current.

Gamma supports both Network and Presentation CLIs. For calls from the customer to Gamma where the call terminates on the PSTN, the SIP FROM field is mapped to the presentation CLI and the SIP P-Asserted-ID is mapped to the network CLI. The behaviour is based on NICC document ND1017 (Table 2), which specifies the mapping from SIP (FROM field) to ISUP (Presentation Number).

To ensure the correct Network CLI is passed into the Gamma network and then forwarded to the PSTN Gamma will insert the customer Network CLI Number in E.164 format into the PA-ID, replacing any value received from the customer CPE.

For calls from the PSTN to the Gamma SIP Trunking endpoint, the SIP FROM field will contain the Presentation Number when available and the P-Asserted-ID field will contain the Network Number when available. If only the Network Number is available, then this will be mapped to both the SIP FROM field and the P-Asserted-ID field.

B-Numbers

B-numbers should be sent to Gamma in the following format:

UK National 0 NSN (National Significant Number) 44 NSN, +44 NSN and 0044 NSN.

International 00 CC NSN and +CC NSN (+CC NSN format is offered on limited connections currently, check with support).

Service and emergency calls no leading 0(s), + or CC (Country Code) to be used.

As a default configuration B-numbers will be presented to the customer including a leading 0, (0 NSN); however, this is flexible, customers can request that a prefix be inserted, or that their number range include a country code.

Number Portability

Number portability for the SIP Trunking service is fully supported and tested. Number Porting changes are currently carried out manually, and it should be noted that BT will only port to a 'live' number; hence the Gamma SIP Trunking endpoints must be configured before the porting can take place.

4.3. Maximum Calls per Second (CPS)

For security reasons, Gamma will also set limits for the maximum calls per second (CPS). The limits dependent on the endpoint design type.

Account Type	Calls/second limit
Single endpoint design	2
Resilient endpoint design	5

If this constraint is reached, Gamma will log and reject calls with a SIP response 486.

4.4. Channel bandwidth

The table below gives an estimate of the bandwidth requirements for VoIP calls using G.711, and G.729a, note that sample periods of 10 and 20 ms only are supported.

The maximum number of concurrent channels = the available bandwidth/total bandwidth, so if for example a customer has a 512 kbps upload line-speed, assuming no contention, using G.729a with a sample period of 20 ms there will be $512/39.2 \sim 10$ usable concurrent channels available. The figures for VoIP using ADSL access are similar.

Codec	Sample period	Encoded sound bandwidth	IP/UDP/RTP overhead	Ethernet overhead	Total bandwidth
G.711	10 ms	64 kbps	32 kbps	30.4 kbps	126.4 kbps
	20 ms	64 kbps	16 kbps	15.2 kbps	95.2 kbps
G.729a	10 ms	8 kbps	32 kbps	30.4 kbps	70.4 kbps
	20 ms	8 kbps	16 kbps	15.2 kbps	39.2 kbps

Table 1 – Suggested MINIMUM VOIP Bandwidth Consumption over Ethernet, Per Channel

Please note that the above represents the best-case, un-contended scenario. Use of other transport protocols (e.g. IPSec), coding mechanisms or contended 'pipes' will further increase the minimum bandwidth required.

Generally, G.729a is the preferred VoIP codec (the algorithm that encodes and decodes analogue voice to and from digital) when access is via ADSL, owing to its efficient use of bandwidth whilst still providing good audio quality.

4.5. Long Duration Calls

Gamma has a policy of terminating any call that exceeds eight hours.

4.6. IP Addressing and DNS

IP version 4.0 is supported. IP Version 6.0 is not supported.

In terms of the CP interaction with Gamma's network, DNS capability, including SRV and A record look-up, is not supported.

4.7. Codecs

Voice encoding can be G.711 A-law or G.729-A with either of two sample periods, 10 ms and 20 ms. Currently the most common sample period is 20 ms although, customers may opt for 10 ms, which introduces less latency but at the expense of greater bandwidth. Only one sample period (10 ms or 20ms) may be provided by a customer. It is important to note that Gamma control the sample period in both the egress and ingress directions of calls made by its customers. Gamma support G.729-A only as a G.729 variant, no other variants of this codec are supported.

Gamma do not support the use of video codecs and customers should make every effort to ensure that no video codecs are included in any SIP requests.

It is recommended that all CP's offer G.711 A-law (20 ms) as a common denominator when negotiating calls, although there is no requirement for this to be the first choice of codec.

Gamma polices the media-stream bandwidth based on the negotiated codec. If a CP exceeds the bandwidth for a specific codec, RTP packets will be discarded and this will result in poor voice quality.

Silence Suppression and Comfort Noise: Gamma support for Silence Suppression and Comfort noise is available to Microsoft Lync connections only.

Ptime:- Gamma do not support the negotiation of codec Ptime. One of the two supported voice sample periods must be selected, via the Gamma Portal, for the desired codec, so eradicating the need for Ptime negotiation. This customer-selected sample period results in a Ptime which is policed by Gamma.

To preserve the quality and continuity of the service, Gamma enforce all the parameters in this section. Customers who do not adhere to these definitions are likely to experience issues with their calls, which may include a loss of service.

06 May 2024

4.8. Session Failover and Endpoint Resilience

The following scenarios will result in an endpoint as being tagged as 'out of service'. In the case of resilient designs, these scenarios initiate failover to alternative sites:

- Destination Unreachable (ICMP unreachable response)
- SIP failure response code
- CAC exhaustion (depending on build type, see section 5 for details)

Destination unreachable

This happens in two ways:

Gamma receives an ICMP unreachable message in response to the INVITE message that it sends out to the endpoint. This could indicate that there is no network route to that destination (i.e. the access method has failed) or the destination is temporarily out of service.

Outgoing INVITEs are retransmitted from Gamma 3 times. If that limit is reached, Gamma will stop trying that endpoint and initiate failover to another endpoint.

In the case of resilient designs, failover is initiated when Gamma concludes that a SIP Trunking endpoint cannot be reached.

SIP Response Codes

When Gamma receives a SIP Final Response, code as detailed in Table 11, in reply to one of its own initial INVITE messages a failover will be initiated in the case of a resilient design. If a SIP response code is received which is not detailed in Table 11 then no failover will occur.

If the SIP response includes a Q.850 reason header then this will take precedence over the SIP response code.

Prevention of Session loss

In order to minimise the impact of failure of network components, it is recommended that within the Channel Partner's network (Proxies and CPE) session timers, as specified by RFC 4028 are implemented. The preferred method for CP to request a change of the refresh time is by means of a SIP error response 422 or a Re-INVITE.

To avoid a high volume of Invite-422-Reinvite iterations at the start of the call, where the SessionExpires value in the originating Invite is less than 1800 seconds (as per RFC 4028), it is recommended this value should not be less than 600 seconds. This will

not prevent Session Interval Too Small responses entirely and it is highly recommended that the CPs that advertise support of the 'timer' feature enable their call-servers to resend the Invite request with the new Session-Expires value upon receipt of a 422 response.

The session refresh time cannot be negotiated by means of UPDATE. The session can be refreshed by means of a Re-INVITE or an UPDATE.

4.9. Customer Premises Equipment

The supply, provisioning and support of all hardware at the customer's site is the responsibility of the Channel Partner.

To ensure compatibility of equipment and ease of installation, Gamma are continually undertaking performance testing with equipment vendors. As such, a list of all currently compatible CPE is provided on the GAMMA portal.

For the CPE devices that have been tested, Gamma suggest Channel Partners contact their equipment vendor for assistance with the installation of this equipment.

Important Note: If connection is required for a device that has not previously been connected to Gamma, the partner can request GAMMA's cooperation with conformance testing to ensure that the device is fully compatible with the Gamma network prior to live provisioning with a customer.

4.10. Network Security

Access to the Gamma SIP Trunk Service from the customers CPE is via IP Authentication and as such, the service will only accept traffic from genuine SIP Trunking endpoints that have been registered on the service.

It is the customer's responsibility to ensure that calls emanating from their endpoint are legitimate and that all practical steps have been taken to avoid fraudulent activity. This would include secure access to their network by means of a Firewall or a Session Border Controller (SBC).

5. Customer Network Design Options

Gamma offers three basic design options as standard for the Gamma SIP Trunk Service.

Single Site – A single site working off a single Gamma SBC High Availability (HA) Cluster. This option provides a service availability of 99.95%.

Active Standby – Dual sites in active / standby mode working off different Gamma SBC HA Clusters.

This enhanced Service offers multiple Customer IP addresses and the Gamma network is Geo Resilient. This option provides a service availability of 99.99% when installed in conjunction with a private interconnect.

Load-share – Dual sites in load share mode working off different Gamma SBC HA Clusters. This enhanced Service offers multiple Customer IP addresses and the Gamma network is Geo Resilient. This option provides a service availability of 99.99% when installed in conjunction with a private interconnect.

In the case of resilient designs (Active Standby or Load-share) one SBC pair is usually located in London and the other in Manchester to provide geographic diversity, two SBC's and two Endpoints is the "standard" design. Gamma advise that, there are limits to the number of SBC's and Endpoints that can be added to a resilient configuration, partners and customers should contact the Gamma Sales or Support organisations to discuss larger configurations than the standard.

5.1. Single Site

This design offers a single site connected to a single Gamma SBC HA Cluster. The connection to the Gamma network may be DSL, Ethernet or a Private connection.

High Availability SBC Cluster

Distributed Softswitch

PSTN

Parameter	Description
Customer Endpoint	Single customer IP address
Channel Limit	Minimum 2 channels , No upper Limit
Call Admission control	Channel limit shared between incoming and outgoing calls
Access	Public or Private
CPS Limit	2 CPS
SBC Gateway	Single Gamma SBC HA Cluster
DDI's	Multiple ranges
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	Automatic and immediate
Availability SLA	99.95%

Table 3 – Single Site Configuration Summary

5.2. Enhanced build

This design offers a single site connected to geographically diverse Gamma SBC HA Clusters i.e. SBC pairs A & B. The connection to the Gamma network may be DSL, Ethernet or a Private connection. This solution offers Gamma connection resilience but no site resilience.

High Availability SBC Cluster

Distributed Softswitch

PSTN

Call Admission Control (CAC)

The Gamma soft switches are configured to route via the SBC A pair as the first choice, and via the SBC B pair as the second choice should the path via the first choice fail.

Both SIP endpoints are configured with a CAC limit which is equivalent to the total channel allocation (e.g. 100 channels). Each channel allocation is shared between incoming and outgoing calls.

It is the CP's responsibility to keep within subscribed bandwidth and the maximum number of concurrent calls allowed. These constraints apply to all calls associated with the CP, regardless of whether they were incoming or outgoing.

CAC exhaustion will result in a non-huntable 486 response.

Fail over and resiliency

Gamma network nodes are configured to route via SBC A as the first choice with second choice routing to SBC B. Failover scenarios are only invoked in the event that a recognized and supported hunt message is received at the Gamma SBC from the end user voice platform. The following scenarios will invoke failover to the secondary endpoint:

Destination Unreachable (ICMP unreachable response)

SIP failure response code which invokes the hunt procedure (Please refer to Table 11)

Please note that a failure condition at endpoint A can increase Post Dial Delay (PDD) by up to 1.5 seconds.

Parameter	Description
Customer Endpoint	Single customer IP address
Channel Limit	Minimum 2 channels , No upper Limit

Call Admission control	Channel limit shared between incoming and outgoing calls
Access	Public
CPS Limit	2 CPS
SBC Gateway	2 Geographically diverse SBC HA Clusters
DDI's	Multiple ranges
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	Automatic and immediate (24 hour delay 5 days after order)
Availability SLA	99.95%

Table 4 – Enhanced Build Site Configuration Summary

5.3. Active Standby

This design offers dual endpoints in active / standby mode working off geographically diverse Gamma SBC HA Clusters i.e. SBC pairs A & B. For this configuration, all traffic will route to the primary endpoint A. In the event of failure all calls will route to the secondary endpoint. ActiveStandby configurations do not support an active and a standby connection on the same SBC.

Standby Site

High Availability SBC Cluster

Distributed Softswitch

PSTN

Active Site

Call Admission Control (CAC)

The Gamma soft switches are configured to route via the SBC A pair as the first choice, and via the SBC B pair as the second choice.

Both SIP endpoints are configured with a CAC limit which is equivalent to the total channel allocation (e.g. 100 channels). Each channel allocation is shared between incoming and outgoing calls.

It is the CP's responsibility to keep within subscribed bandwidth and the maximum number of concurrent calls allowed. These constraints apply to all calls associated with the CP, regardless of whether they were incoming or outgoing.

In the event that Endpoint A is in service but sends back a hunt-able SIP response (e.g. 408, 503, 504) then calls will be presented to Endpoint B and those calls will not be accounted for in further CAC restriction at Endpoint A. For example; If endpoint A fails and 'x' number of calls are setup to endpoint B and then Endpoint A recovers for the duration of the 'x' calls then the total CAC possible would be 'x' + 100 calls.

CAC exhaustion will result in a non-hunnable 486 response.

Please note, Gamma expects the standby channel allocation to be within 50% of the active channels on Active/Standby and this is to ensure we can protect the integrity of the Gamma network and to protect a flood of traffic towards our SBCs if calls are failing to the active SIP trunk.

Fail over and resiliency

Gamma network nodes are configured to route via SBC A as the first choice with second choice routing to SBC B. Failover scenarios are only invoked in the event that a recognized and supported hunt message is received at the Gamma SBC from the end user voice platform. The following scenarios will invoke failover to the secondary endpoint:

Destination Unreachable (ICMP unreachable response)

SIP failure response code which invokes the hunt procedure (Please refer to Table 11)

Please note that a failure condition at endpoint A can increase Post Dial Delay (PDD) by up to 1.5 seconds.

Parameter	Description
Customer Endpoints	2x customer IP addresses on same site or different sites
Channel Limit	Minimum 2 channels , No upper Limit
Call Admission control	Channel limit shared between incoming and outgoing calls Theoretical channel maximum = 200% of channel allocation
Fail over	100% of channel allocation in fail over scenario
Access	Public or Private
CPS Limit	5 CPS

SBC Gateway	2 Geographically diverse HA Clusters
DDI's	Same DDI ranges shared across both endpoints
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	10 day lead time
Availability SLA	99.99%

Table 5 – Active Standby Configuration Summary

5.3.1 Resilience+

The Resilience+ account is designed to offer two SIP endpoint connections where each endpoint is active to selected DDI's whilst standby resilience is provided by the other endpoint. Resilience+ accounts offer dual live sites with dual fail over options.

High Availability SBC Cluster

Distributed Softswitch

PSTN

Active Site

Active Site

Allocated DDIs

Allocated DDIs

The Resilience+ design offers dual endpoints both in active-standby mode working off geographically diverse Gamma SBC HA Clusters. For this configuration, individual DDIs or DDI ranges can be allocated to the desired endpoint and traffic route accordingly. In the event of connection or site failure all calls will route to the alternate endpoint.

Benefits of the Resilience+ account include the ability to define both the DDI ranges and channel allocations at each site. In the event that communication to either a site is unavailable, then the remaining site will receive all related traffic. Resilience+ accounts do not have to be symmetric e.g.

in a 100 channel deployment channels can be allocated in a 60/40, 65/35, etc. configuration if desired but must be within 50% of the primary endpoint.

Call Admission Control (CAC)

The Gamma soft switches are configured to route via the SBC A pair as the first choice, and via the SBC B pair as the second choice.

Both SIP endpoints are configured with a CAC limit. The CAC limit on each endpoint does not need to be the same provided the smaller limit is greater or equal to 50% of the larger limit. For example, 60:40 is allowed but 80:20 is not allowed. Each channel allocation is shared between incoming and outgoing calls.

It is the CP's responsibility to keep within subscribed bandwidth and the maximum number of concurrent calls allowed. These constraints apply to all calls associated with the CP, regardless of whether they were incoming or outgoing.

In the event that Endpoint A is in service but sends back a hunt-able SIP response (e.g. 408, 503, 504) then calls will be presented to Endpoint B and those calls will not be accounted for in further CAC restriction at Endpoint A. For example; If endpoint A fails and 'x' number of calls are setup to endpoint B and then Endpoint A recovers for the duration of the 'x' calls then the total CAC possible would be 'x' + 100 calls.

CAC exhaustion will result in a non-hunttable 486 response.

Please note, Gamma expects the standby channel allocation to be within 50% of the active channels on Resilience+ builds. This is to ensure we can protect the integrity of the Gamma network.

Fail over and resiliency

Gamma network nodes are configured to route via SBC A as the first choice with second choice routing to SBC B. Failover scenarios are only invoked in the event that a recognized and supported hunt message is received at the Gamma SBC from the end user voice platform. The following scenarios will invoke failover to the secondary endpoint:

Destination Unreachable (ICMP unreachable response)

SIP failure response code which invokes the hunt procedure (Please refer to Table 11)

Please note that a failure condition at endpoint A can increase Post Dial Delay (PDD) by up to 1.5 seconds.

Parameter	Description
Customer Endpoints	2x customer IP addresses on same site or different sites
Channel Limit	Minimum 2 channels , No upper Limit

Call Admission control	Channel limit shared between incoming and outgoing calls Theoretical channel maximum = 100% of channel allocation
Fail over	Channel allocation of active endpoint in fail over scenario
Access	Public or Private
CPS Limit	5 CPS
SBC Gateway	2 Geographically diverse HA Clusters
DDI's	Same DDI ranges shared across both endpoints
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	10 day lead time
Availability SLA	99.99%

Table 6 – Active Standby Configuration Summary

5.4. Load Share

This design offers dual endpoints in a load-share mode working off geographically diverse Gamma SBC HA Clusters i.e. SBC pairs A & B. For this configuration, traffic will be shared using a load share algorithm to ensure equal distribution between endpoints over a period.

High Availability SBC Cluster

Distributed Softswitch

PSTN

Active Site

Active Site

TSS4

All DDIs

Call Admission Control (CAC)

Each SIP endpoints is configured with half the total channel allocation (e.g. 50 out of 100 channels). Each channel allocation is shared between incoming and outgoing calls.

06 May 2024

In cases where the call control constraint (CAC limit) is exceeded at an SBC, excess traffic will overflow/re-route to the alternative SBC if additional capacity is available. To ensure this operation, CAC exhaustion on both SBC A and SBC B will send a 503 SIP response back to the Gamma network to ensure it hunts between the two SBC clusters. This configuration ensures 100% of the channel allocation is available at any time, except in outage cases when only 50% of channel allocation would be available.

Fail over and resiliency

Gamma network nodes are configured to load share traffic across both SBC nodes. Failover scenarios are only invoked in the event that a recognized and supported hunt message is received at the Gamma SBC from the end user voice platform. The following scenarios will invoke failover and force traffic to the alternative endpoint:

CAC exhaustion

Destination Unreachable (ICMP unreachable response)

SIP failure response code which invokes the hunt procedure (Please refer to Table 11)

In the event of SBC or customer connectivity failure, traffic will route to the alternative site. Channel allocation will remain at ½ the total call allowance.

Parameter	Description
Customer Endpoints	2x customer IP addresses on same site or different sites
Channel Limit	Minimum 2 channels , No upper Limit
Call Admission control	Channel limit shared between incoming and outgoing calls Theoretical channel maximum = 100% of channel allocation
Fail over	50% of channel allocation in fail over scenario
Access	Public or Private
CPS Limit	5 CPS
SBC Gateway	2 Geographically diverse HA Clusters
DDI's	Same DDI ranges shared across both endpoints
Codecs & Packetisation	G.711 a-law or G729 at 10 ms or 20ms
Provisioning SLA	10 day lead time

Availability SLA	99.99%
------------------	--------

Table 7 – Load Share Configuration Summary

5.5. Failover examples

Gamma resilient SIP Trunking solutions rely on customer CPE response codes in order to trigger a hunt action i.e. an attempt to deliver an Inbound call to the customers secondary endpoint in a failure scenario. Gamma will also trigger a hunt action if no response is received from the customer CPE due to circumstances such as a total loss of IP connectivity.

In order that the customer is able to configure their CPE to interoperate correctly with Gamma, the following response codes are required by Gamma in order to trigger a inbound hunt action. This also outlines what Gamma suggests the customer CPE reacts to in the event that Gamma has reason to deliver a SIP failure response code to the customer platform.

Scenario 1

The End user has a Load-Share resilient SIP Trunking build over 2+ SIP trunk end points. Gamma’s policy for building and deploying such resilient designs is that each endpoint is built back to a geographically diverse SBC HA pair, situated in Manchester and London. It can be the case though that in order to support end user requirements Gamma builds more than one endpoint back to the same SBC HA pair. Active-Standby configurations do not support standby connections on the same SBC as active connections

If resiliency is setup between 2+ endpoints built back to the same Gamma SBC pair, Gamma will force a hunt response (inbound calls – Gamma to end user) if it receives one of the following SIP response codes from the CPE:

SBC Hunt response codes (Grid 1):

400	402	405	406	408	409	411	413
414	415	420	480	482	483	485	487
488	500	502	503	504	505	580	606

Scenario 2

The End user has a resilient SIP Trunking build, Active/Standby or Load-balanced over 2+ SIP trunk end points. The solution uses the standard Gamma implementation method whereby each endpoint is configured on a separate Gamma SBC HA pair.

In this instance the Gamma SBC HA pair will pass back the SIP error response it receives from the end user CPE. The response is then handled by the top layer of the Gamma SIP Trunking resilient mechanism. The Gamma Soft switch layer will force a hunt response if it receives one of the following SIP response codes:

Soft switch Hunt response codes (Grid 2):

400	408	480	481	500	502	503	504
-----	-----	-----	-----	-----	-----	-----	-----

Scenario 3

The End user has a resilient Load-Share SIP Trunking build, Load-Shared over 3+ SIP trunk end points which form a mixture of Scenario 1 and 2 above. As an example the end user has 2 SIP trunk end points built back to Gamma SBC HA pair 1 and a 3rd end point built back to Gamma SBC HA pair 2. This scenario is not supported for the Active-Standby mode as such configurations do not support standby connections on the same SBC as active connections.

In this instance customer site A and A/B in the diagram above (Blue) will have CPE DR message requirements as per Scenario 1. Customer site B/C will have Inbound DR message requirements as per Scenario 2.

Customer site A is the primary Inbound delivery trunk for a particular call. Customer site A fails and sends a 408 SIP response code.

Customer site A is the primary Inbound delivery trunk for a particular call. Customer site A fails and send a 408 SIP response code. Customer site A/B also fails returning a 503 SIP response code.

6. Network Access and Connectivity Options

SIP Trunking endpoints can be configured as both public and private IP addresses allowing access to Gamma SIP Trunking services via public internet or private interconnect. This access can be provided by Gamma or Third Parties with the following options:

6.1. Public Internet

The customer's CPE (typically an IPBX supporting SIP) is defined as an 'endpoint' within the Gamma SBC, with each endpoint capable of having a number of devices connected to it.

A static public IP address assigned by the customer's ISP will be configured and used to authenticated the endpoint, providing duplex interconnection to the PSTN.

Access Control – Configuration of NonGamma access routers

Network administrators must ensure that the SIP Trunk IP addresses and ports (both directions) are available and not blocked by firewalls. Each new SIP endpoint you create will be built against a given Gamma SBC, which will have a specific signalling & media IP which you will need to configure against your Router, SBC/PBX and firewall. These specific IP's and the ports will be confirmed once the new order has gone live and you have received your order confirmation email. If these ports are not opened (i.e. a customer or network-based firewall is blocking them), or IP addresses allowed, your SIP Trunk will not function correctly.

06 May 2024

If you are deploying a larger SIP environment, you may wish to whitelist ALL Gamma SBC IP's to prevent the need to update the Router, SBC/PBX and firewall at a later point. Below are the details of each SBC IP subnet which you will need in order to achieve this, as this will cover all Gamma SBC signalling & media IP addresses and ports.

Gamma recommends that only trusted IPs are permitted to send and receive traffic via port 5060 and 5080. The ports the SIP endpoint will use can also be changed via the Gamma Portal to any port of your choosing. If you choose to do this you will need to consider updating your Router, SBC/PBX and firewall to also accommodate this change.

Transport Protocol	IP Subnet	Function
TCP	83.245.6.0 /24	SBC SIP signalling
TCP	88.215.56.0 /21	SBC SIP signalling
TCP	88.215.54.0 /23	SBC SIP signalling
UDP	88.215.56.0 /21	SBC SIP signalling
UDP	88.215.54.0 /23	SBC SIP signalling
UDP	88.215.56.0 /24	SBC SIP signalling
TCP	88.215.56.0 /24	SBC SIP signalling
TCP	88.215.54.0 /23	SBC SIP signalling
UDP	88.215.48.0 /20	SBC SIP signalling
TCP	88.215.48.0 /20	SBC SIP signalling
TCP	88.215.48.0 /25	SBC SIP signalling
UDP	88.215.48.0 /20	SBC RTP Traffic
UDP	83.245.6.0 /24	SBC RTP Traffic
UDP	151.2.128.0 /19	SBC SIP signalling
TCP	151.2.128.0 /19	SBC SIP signalling
UDP	151.2.128.0 /19	SBC RTP Traffic

6.2. Private Interconnect

In order to assuage perceived security and quality concerns, Gamma offers improved access options:

Private interconnection via the Gamma IP Assured service

Private interconnection via Ethernet

Private interconnection to Gamma into POP (Layer 2 VLAN)

Access via Private interconnection is possible at the following Gamma peering points:

Telecity 2, 8/9 Harbour Exchange Square, London, E14 9GE – Rack 3V24

Telehouse East, Coriander Avenue, London, E14 2AA – TFM51 Rack E18

Redbus, 6/7 Harbour Exchange Square, London, E14 9HE – Rack 8R19 Floor 8

Telehouse North, Coriander Avenue, London, E14 2AA – TFM15 Cab C13

Eplison Global Hubs, 2nd Floor, 69-77 Paul Street, London, EC2A 4NW – Meet Me Room (MMR)

City Lifeline, 80 Clifton Street, London, EC2A 4HB – Citrus Suite, 2nd Floor, Rack B4

Telecity Powergate, Unit 1, Powergate Business Park, Volt Avenue, London, NW10 6PW – Meet Me Room (MMR)

Telecity, Kilburn House, Lloyd Street, Manchester, M15 6SE – Rack AH4

Telecity, Joule House, 76 Trafford Wharf Road, Manchester, M17 1HE – Rack S7A07

Equinix – Rack LD04:01:C01 (Rack LD05 may also be cross connected to Rack LD04)

Network Demarcation

For Private interconnection the Gamma Telecom demarcation point resides at the internal fibre cross connect presentation at the customer rack location with the Data centre. It is the customers' responsibility to identify (localise) and resolve problems affecting IPT services caused by the customer premises equipment (CPE) and local infrastructure beyond this demarcation.

Quality of service

It is not necessary for the customer to mark traffic on the egress to their network before it enters the Gamma device terminating the internal cross connect and Gamma will not deliver marked voice traffic (Signalling or Media) to the customer.

Resilient Connectivity

For maximum resilience it is required that customers interconnect at two diverse peering points. All peering point combinations are diverse with the exception of the following combinations: Telecity 8/9 and;

Telecity Powergate

Connection Types

Connection Types include copper, single or multi-mode fibre and bandwidths ranging from 10Mbps to 1Gbps. Interconnect port types include Layer 3 BGP, Layer 2 VLAN or Layer2 801q VLAN. For improved connectivity resilience at each peering point, CP's should consider diverse connections as opposed to single connections.

IP Addressing and Gamma Ethernet connectivity

For SIP Trunking customers connecting via Gamma Ethernet, Gamma allocated a private /29 subnet for use on the customer side of the Gamma router. This /29 subnet includes:

- 1 IP out of the range for the customer to configure their CPE
- 1 IP out of the range as the Customer Default Gateway

Please note: The Gamma SIP Trunking Signalling and Media Gateway address is in a different range. Customer will therefore need to configure their CPE to use the Customer Default Gateway as the route to the Gamma signalling address.

7. Protocol & Signalling support

Gamma can offer SIP signalling transport over UDP. The standard is UDP. In cases where PBXs use TCP signalling, SIP Proxy server's/IP gateways are required to convert to UDP on the customer's premises.

7.1. RFC Support

The Gamma SIP Trunking service supports the following RFC's. Full compliance is subject to differences in interpretation, interoperability constraints and the exceptions noted below.

RFC	Supported
RFC 2327 Session Description Protocol	Yes

RFC2543 SIP: Session Initiation Protocol	Yes, Putting Media streams on Hold, Indicate the IP in SDP message when "call-hold" mechanism is used according RFC 2543: Gamma will support receiving either the actual IP or 0.0.0.0 if interworking to TDM. If the incoming/outgoing route is via a SIP interconnect partner this may not be the case.
RFC 2833 – RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	Yes
SIP RFC 3261- SIP Messages, Headers & Protocol	Yes
RFC 3262 – Reliability of Provisional Responses in SIP:	Yes
RFC 3264 – An offer/answer model with SDP:	Yes
SIP RFC 3311 – SIP Update Method	Yes (only during unconfirmed dialogue). Re-INVITE should be used when dialogue is in confirmed state.
SIP RFC 3325 – Privacy extensions to SIP for Asserted Identity within trusted networks	Yes
SIP RFC 3326 – Reason-Header Field for SIP	Yes
RFC 3398 – ISDN to SIP Mapping:	Yes
RFC 3551 – RTP Profile for audio:	Partial, Gamma will only support G711, G729 and G729A codecs
RFC 4028 Session Timers in the Session Initiation Protocol	Yes
NICC ND1017:2006/07. TSG/SPEC/017. Interworking between Session Initiation Protocol (SIP) and UK ISDN User Part (UK ISUP)	Yes

Table 8 – Gamma SIP Trunking reference RFCs and other Standards

7.2. Signalling and Encoding

Gamma SIP Trunk Service provides SIP signalling as a method for Communication Providers to inter-connect with Gamma's VoIP network, supporting VoIP to VoIP calling as well as calls to/from the PSTN.

Gamma SIP Trunk Service supports the transport of SIP signalling messages using UDP. SIP messages sent using TCP(except for MS Lync), TLS, SCTP and IPSEC are not supported at present.

SIP V2 is supported between the SBC and the customer CPE. The SIP standard is documented in the Internet Engineering Task Force (IETF) RFC 3261.

Please note that this service does not support H.323, SIP-I, SIP-D and SIP-T.

Format of the SIP INVITE Field

The SIP header requirements in the INVITE packets originated from the CPE should be set as follows:

Request URI must contain the B-number followed by the assigned Gamma SIP gateway IP address:

INVITE sip:01618700000@"IP Address";user=phone SIP/2.0

The FROM header must contain your public facing IP address and originating CLI:

FROM: <sip:+441618777148@"IP Address">; tag=3528194925-554920

The TO header must contain the assigned Gamma SIP gateway IP address and the B-number*:*

To: <sip:01618700000@"IP Address";user=phone>

- For network security reasons, the source IP of any RTP media streams must match the public IP address provided in the SDP payload. Media streams with source IP addresses not provided in SDP payload will be discarded, resulting in loss of audio.

Traffic on the following ports must be forwarded through relevant routers and firewalls on the customer premises to allow access to the Gamma SIP Trunking Network:

UDP Port 5060 egress/ingress

UDP all ports between 6000 – 40000 egress/ingress

For ingress calls the INVITE Request Line must contain a SIP URI.

For egress calls from Gamma to the customer the INVITE Request Line will contain a SIP URI.

Example of the initial SIP INVITE

The SIP gateway here is 88.215.61.195 – this will be stated in the SIP Trunking order confirmation.

The CPE IP address is 88.215.25.5 – the public IP address with which Gamma's SBC communicates. This address is defined in the Gamma SIP Trunk Service order, and can be updated via the Gamma Portal. The fields highlighted below must contain the CPE IP address. If the PBX is operating behind a NAT these addresses will need to be NAT'ed by a SIP aware device e.g. an SBC, a router with an ALG, the PBX itself via STUN.

SIP Message

INVITE sip:01412485779@88.215.61.195 SIP/2.0

Via: SIP/2.0/UDP 88.215.25.5:5080;branch=z9hG4bK-a8b33135

From: "+441414040025" <sip:+441414040025@88.215.61.195>;tag=9fa8f5c74acc1965o0

To: <sip:01412485779@88.215.61.195>

Call-ID: [9899ceef-2d38d25d@192.168.1.8](#)

CSeq: 101 INVITE

Max-Forwards: 70

Contact: "+441414040025" [sip:+441414040025@88.215.25.5:5080](#)

Expires: 240

User-Agent: Linksys/SPA942-6.1.5(a)

Content-Length: 250

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, PRACK, REFER

Supported: 100rel, replaces

Content-Type: application/sdp

SDP v=0

o=- 14849 14849 IN IP4 192.168.1.8 s=-

```
c=IN IP4 88.215.25.5 t=0 0 m=audio 7776
RTP/AVP 8 18 101 a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729a/8000 a=fmtp:18
annexb=no a=rtpmap:101 telephone-
event/8000 a=fmtp:101 0-15 a=ptime:20
a=sendrecv
```

Explanation:

The Via header (the topmost via if there are multiple) is used in conjunction with the layer 3 IP address for authentication. If the address is unknown to our SBC (e.g. LAN address) it will respond 403: Forbidden.

The Contact header advises our SBC where to respond to. If this is a LAN address, or some other address which you're not expecting traffic on, the 2-way dialog will be disrupted and calls will not setup correctly.

The c= parameter in the SDP (connection address) is the address to which your user agent is requesting media (RTP) is sent. Again, this needs to be reachable by Gamma's SBC. If this is not NAT'ed, and you send a LAN IP address, the call may setup OK but you will get one way speech (with the remote party not heard by the SIP Trunking user)

7.3. Supported SIP methods and responses

The list of supported SIP methods is detailed below.

Supported SIP methods

Method	Extent of Support	Notes
ACK	Full, receive and transmit	
BYE	Full, receive and transmit	The "Reason-Header" field in BYE or CANCEL message is preferred but not essential
CANCEL	Full, receive and transmit	The "Reason-Header" field in BYE or CANCEL message is preferred but not essential

INVITE	Full, receive and transmit	
OPTIONS	Full, receive and transmit	
PRACK	Full, receive and transmit	
UPDATE	Full, receive and transmit	UPDATE supported only during an unconfirmed dialogue

Table 9 – Supported SIP methods

Supported SIP Responses

Response	Extent of Support	Notes
100 TRYING	Full, receive and transmit	
180 RINGING	Full, receive and transmit	
181 Forwarded	Minimal, receive only	
183 Session Progress	Full, receive and transmit	In cases of TDM interworking then a 183 session progress will be sent when the outgoing MGW is seized regardless of the subscriber state. In cases where the outgoing route is towards a SIP interconnect partner this may not be the case.
200 OK	Full, receive and transmit	Gamma will include SDP in 200-Ok answer message which will be the same as any SDP previously sent in a 18x message
400 Bad Request	Full, receive and transmit	
403 Forbidden	Full, receive and transmit	
404 Not found	Full, receive and transmit	

405 Method Not Allowed	Minimal, receive only	
406 Not Acceptable	Minimal, receive only	
408 Request Timeout	Minimal, receive only	
415 Unsupported Media Type	Full, receive and transmit	
422 Session Timer Interval Too Small	Full	
480 Temporarily Unavailable	Full, receive and transmit	
481 Call Leg/Transaction Does Not Exist	Full, receive and transmit	
482 Loop Detected	Full, receive and transmit	
483 Too Many Hops	Full, receive and transmit	
484 Address Incomplete	Full, receive and transmit	
486 Busy Here	Full, receive and transmit	
487 Request Terminated	Full, receive and transmit	
488 Not Acceptable Here	Full, receive and transmit	
491 Request Pending	Full, receive and transmit	
500 Internal Error	Full, receive and transmit	
501 Not Implemented	Full, receive and transmit	
502 Bad Gateway	Minimal, receive only	
503 Service Unavailable	Full, receive and transmit	
504 Server Time-out	Full, receive and transmit	
600 Busy Everywhere	Minimal, receive only	
603 Decline	Minimal, receive only	
604 Does Not Exist	Minimal, receive only	
606 Not Acceptable	Minimal, receive only	

Table 10 – Supported Responses

7.4. Hunt-able SIP Responses

The following SIP responses when sent back from SITE A (Active/Standby) or either SITE (Load Balanced), will cause the network to hunt to the next available customer endpoint.

SIP Status Code rec'vd	Cause/ CNA/ Q850	Hunt-able SIP response
400 (Bad Request)	NONE	Yes
401 (Unauthorised)	NONE	
402 (Payment Required)	NONE	
403 (Forbidden)	NONE	
404 (Not found)	NONE	
404 (Not found)	1 (Unallocated Number)	
405 (Method Not Allowed)	NONE	
406 (Not Accepted)	NONE	
407 (Proxy Auth. Required)	NONE	
408 (Request Timeout)	NONE	Yes
410 (Gone)	NONE	
413 (Req.Entity Too Long)	NONE	
414 (Req. URI Too Long)	NONE	
415 (Unsupported Media Type)	NONE	
416 (Unsupported URI Scheme)	NONE	
420 (Bad Extension)	NONE	
421 (Extension required)	NONE	

423 (Interval Too Brief)	NONE	
480 (Temporarily Unavailable)	NONE	Yes
481 (Call / Transaction Not Exist)	NONE	Yes
482 (Loop Detected)	NONE	
483 (Too many Hops)	NONE	
484 (Address Incomplete)	NONE	
484 (Address Incomplete)	28 (Address Incomplete)	
485 (Ambiguous)	NONE	
486 (User Busy)	17 (User busy)	
486 (User Busy)	NONE	
487 (Request Terminated)	NONE	
488 (Not acceptable Here)	NONE	
491 (Request Pending)	NONE	
493 (Undecipherable)	NONE	
500 (Server Int. Error)	NONE	Yes (with q.850 Reason Header containing reason 41)
500 (Server Int. Error)	34 (No Channel Available)	
500 (Server Int. Error)	41 (Temporary Failure)	Yes (with q.850 Reason Header containing reason 41)
500 (Server Int. Error)	42 (Switching Equip. Cong)	
502 (Bad Gateway)	NONE	Yes

503 (Service Unavailable)	NONE	Yes (with q.850 Reason Header containing reason 41)
503 (Service Unavailable)	41 (Temp fail)	Yes (with q.850 Reason Header containing reason 41)
504 (Server Timeout)	NONE	Yes
600 (Busy Everywhere)	NONE	
603 (Decline)	NONE	
604 (Does Not exist Anywhere)	NONE	
606 (Not Acceptable)	NONE	

Table 11 – Hunt-able SIP responses

8. Fraud Management Service description

The Fraud Management System (FMS) feature allows Gamma SIP Trunk channel partners to protect themselves from fraudulent activity from endpoints that have fallen victim to hacking or excessive unauthorised call spends. The feature allows partners to pre-set individual call limits against specific IPDC endpoints and have automatic call barring invoked if these thresholds are breached.

There is mounting awareness within the partner community concerning VoIP security; by introducing this configurable fraud management feature, Gamma is able to address these concerns in a simple and effective manner. The partner will not be responsible for any fraudulent over-spend above the configured threshold limit.

The feature is entirely under the direct control of the channel partner, accessed exclusively from the Gamma Portal and does not require any input from Gamma.

It is available to all existing channel partners that currently manage their endpoints via the Portal.

8.1 Functionality Overview

Once logged into the Gamma portal, the partner can subscribe to the FMS functionality on a per SIP Trunking (IPDC) end-point level.

For existing endpoints, the process works as follows:

Identify the relevant endpoint on the portal

Select Fraud Management from the Operations drop down menu (order summary page)

Configure a 24hr and/or 7 Day max spend limit for this endpoint Set Email/SMS notification address.

Save these settings; the Fraud Management System is now active

The system will now monitor the end user spend by systematically polling their CDRs and rating them accordingly. The accumulated total from the notional start time (i.e when the FMS was started) will be monitored. When the total reaches the warning threshold (typically configured at 85% of maximum spend), the system will generate a warning Email and SMS (where configured).

The partner can then choose to take some form of action, investigating with the end-user or raising the spend limit etc. If no alternative action is taken, the system will continue to monitor the spend until it breaches either the 24hr or 7 Day tracking threshold, at which point an 'All Calls Barred' action will be automatically placed on the end point and no further outbound calls will be possible (see note 1).

The system will automatically generate a further email and SMS (where configured) detailing the fact that this endpoint has breached its limit together with the current spend before call barring became effective. The email will also contain a summary of the most recent call records

Once the endpoint has breached its limit and call barring has been applied, it will remain in this state until the call barring is removed by the partner.

Note 1: Calls to the Emergency Services will be unaffected.

Note 2: The operational requirements including scheduled polling, mediation and activation logic mean that the call barring can take up to an hour to take effect. The final spend may therefore overrun the configured spend limit; a fact that should be 'factored in' when setting individual spend limits.

Note 3: All calls originating from the endpoint will be included in the aggregated spend.

8.2 Functional Schematic

8.3 Charges

This feature is Free of Charge (FOC) to Channel Partners.

8.4 Status Information

The current Fraud Alert Status for the endpoint is displayed on the Portal via the order list and can be either:

Active	The FMS feature has been activated and is monitoring the call spend
Suspended	The endpoint has been suspended with all Call Barring applied
None – Set	The FMS feature has not been activated

Service Details

Health Check

Service

Numbers

Customer

History

Service Status

Call Barring

Fraud Management

Access

Advanced Diagnostics

All subsequent changes to the status will be reflected here.

8.5 Terms and Conditions

If an endpoint had the FMS feature set enabled, it will be applied and charged to all channels on the endpoint.

Gamma will only waive charges for calls that breach the configured threshold (see note 2) where they can be show to be fraudulent.

Network Call Diverts are excluded from the Fraud Management Service and do not form part of the aggregated call spend for this purpose. Charges for any Network Call Diverts and associated calls will be chargeable to the Channel Partner in all circumstances.

We reserve the right to withhold crediting in instances of multiple fraud management barring events on the same Endpoint

The use of the FMS feature is subject to the above terms and conditions and to the general provisions of the Channel Partner's supply agreement (Telecommunications Services Agreement or Switchless Resale Agreement). In the event of a conflict with the supply agreement the above terms and conditions shall apply.

8.6 Configuration

New IPDC order

During the Portal IPDC order process, the FMS feature is presented as part of the standard configuration option. This is an opt-out service as seen by the pre-ticked box at the top of the configuration screen (see fig 1).

If the box is un-ticked, a pop-up on the screen will remind the user that they will now be responsible for any fraudulent and/or un-authorised spend on this endpoint.

This screen captures all the information needed to configure Fraud Management for this endpoint. Note also that there are pre-populated default values which should be modified to suite the requirements of each individual endpoint.

Daily Spend Limit

The daily spend limit is a rolling 24 hr aggregation of call charges across all channels on that endpoint, the time starts when the endpoint is successfully commissioned as part of a new order or when the feature is configured and then 'saved' on an existing endpoint.

The 24 hr clock will re-set if the threshold is breached and subsequently has the blocking removed.

Weekly Spend Limit

The weekly spend limit is a rolling 7-day aggregation of call charges across all channels on that endpoint, the time starts when the endpoint is successfully commissioned as part of a new order or when the feature is configured and then 'saved' on an existing endpoint.

The 7-day clock will re-set if the threshold is breached and subsequently has the blocking removed.

In both cases, a configurable threshold alert warning can be configured to warn if either limit is getting close to breach. e.g. at 85% of maximum call spend.

Access/Edit Fraud Management for an existing Endpoint

For existing endpoints, the Fraud Management System is accessible by clicking on the "Fraud Management section of the Service screen (as diagram above).

Selecting this option will reveal the configuration page (as below) with the option to set-up a new or modify an existing thresholds setting.

Gamma SIP Trunks - Configure Fraud Management

Fraud Management Settings

**Terms and Conditions**
This order is subject to the terms and conditions set out in section 5 of the Gamma SIP Trunks Fraud Management Service Description, which can be accessed on the 'Gamma SIP Trunks' section of the Gamma Knowledge Base, and your supply agreement with Gamma Telecom Ltd.

☒ Enable Fraud Management

☒ Enable Daily Limit

Daily Limit (£): *

Email Address(es): *

Warning Threshold (%): *

☐ Send SMS

☒ Enable Weekly Limit

Weekly Limit (£): *

8.7 Partner Notification of Limit Breach

If the endpoint exceeds either the 24 hour or 7 Day limit, the endpoint will be automatically barred from making any outbound calls, (with the exception of emergency service calls). An email (Fig 4) will then be sent from 'Gamma Fraud Management Systems' containing the following details and will be delivered to the address configured in the original notification alert:

- Action: All Calls Barred
- Threshold Breach Period
- Endpoint Identification
- Total Call Duration
- Total Call Cost

Total Number of Calls

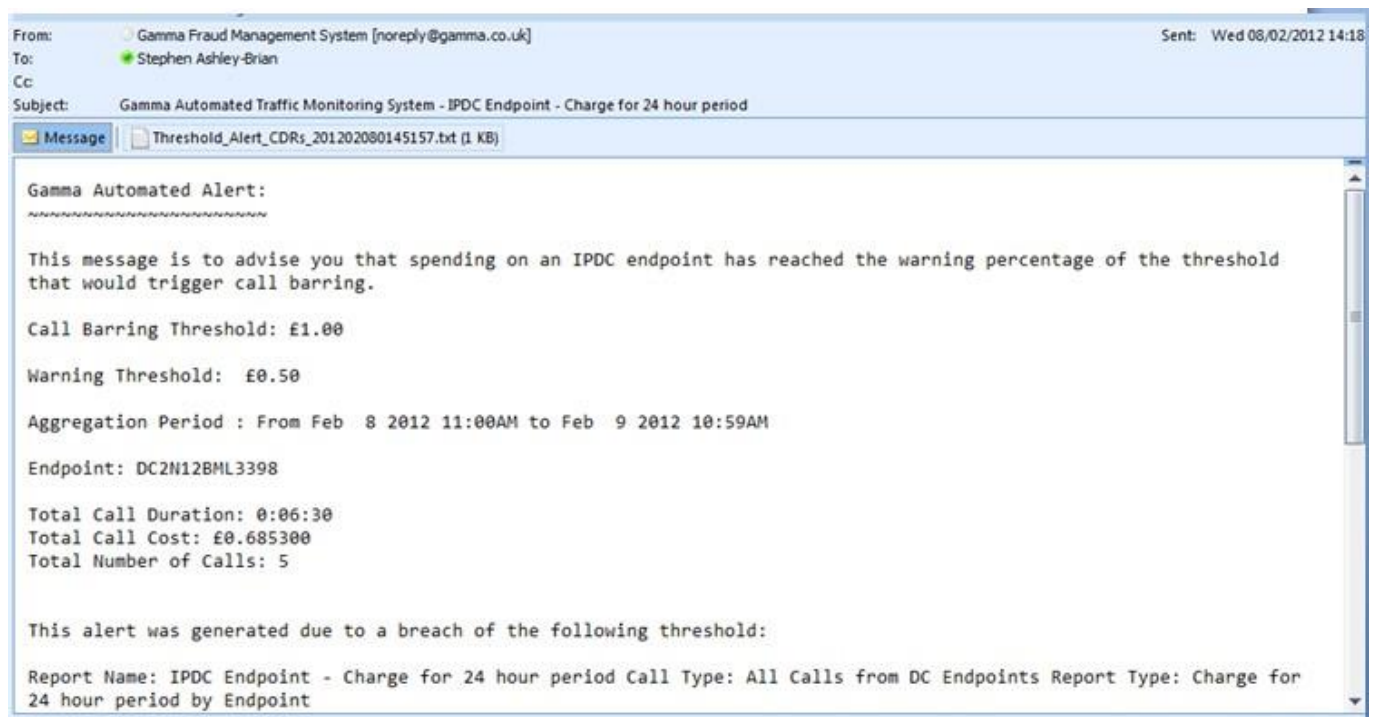
The email will contain an attachment with the relevant CDRs for the period covered. This detail can be used to assist in the determination of whether fraudulent calls have been made.



In addition, if configured on the FMS, a SMS will also be sent detailing the following:

- Action: All Calls Barred
- Threshold Breach Period
- Endpoint Identification
- Total Call Duration
- Total Call Cost

A warning email and SMS will also be sent prior to call barring if the threshold alert warning has been configured, (see below).



End User Notification

It is the partner's responsibility to inform the end user as to the reason that Call Blocking has been applied to their account. End users will receive a 'fast busy' when attempting to make outbound calls. In a future release, call attempts will be diverted to a recorded announcement instructing them to contact their service provider.

Resetting after Breach

In order to remove call blocking from an endpoint following automated call barring, the partner logs onto the portal where they will see the current status of the endpoint: i.e. suspended.

After selecting Fraud Management from the service screen, clicking on 'Un-Suspend This Endpoint' will remove the call barring from this endpoint and restart the aggregation metrics as determined by the previously configured thresholds.

The partner can then choose to modify the spend limits accordingly.

9. Dialler Policy

Gamma does not accept any Dialler traffic onto its SIP trunking service and will take efforts to remove such traffic if/when detected.

This position is based on the operational need to safeguard our network and ensure that optimum service levels remain available to all of Gamma's customers across our SIP Trunking services. In addition, the following Ofcom guidelines <http://stakeholders.ofcom.org.uk/consultations/silent-calls/statement/> regarding nuisance, silent and abandoned calls would be considered by Gamma to be a regulatory requirement to be adhered to by any signatory to our contracts.

For clarity, Gamma considers acceptable traffic to have an Average Call Hold Time (ACHT) of greater than 50 seconds and an Answer Seize Ratio (ASR) of greater than 60%.

In addition, please be aware that Gamma actively monitors all SIP traffic and will respond to endpoints that exhibit 'dialler like' call patterns. In the first instance, this will mean contacting the customer to help resolve the situation by reducing capacity and agreeing a resolution timeframe; however this does not preclude Gamma from barring the endpoint without notification in extreme circumstances.

10. Provisioning

Please refer to the SIP Provisioning and In Life Changes guide for help on provisioning and the Gamma Customer Service Plan for provisioning lead times.

11. Fault Handling, Escalation, and Reporting

Please see the SIP Technical Support guide for help with faults and the Gamma Customer Service Plan for provisioning lead times.

12. Billing

Please refer to the Gamma SIP Trunk Service Billing Description for CDR formats and billing processes. This information is available on the Gamma Portal under “Billing Home”

13. Calls Between the Emergency Handling Centre and Emergency Authority

In the UK calls to the Emergency Services (999/112) are handled by an Emergency Handling Centre (EHC) operated by BT. The call is answered by the centre and then, on the basis of the address held in the EHC’s database or provided by the caller, is then forwarded to the correct regional

Emergency Authority (EA). This forwarded leg of the call will generally be made to the geographic number used by the EA to receive this type of call directly into their own emergency control room. Additional information is conveyed from the EHC to the EA by means of the Enhanced Information Service for Emergency Calls (EISEC) which uses additional digits appended to the CLI as a pointer to access a database entry populated by the EHC. The EISEC is a service operated by BT.

Gamma cannot support the hosting of the EA geographic number on a SIP trunk (or using the Horizon platform) at this time due to the limitations detailed below.

At this time there is no standardised way within the UK to assert ‘Priority’ to the forwarded call from the EHC to the EA in the SIP signalling system. These calls are not easily distinguishable by destination number.

At this time the EISEC service is not guaranteed to consistently work over SIP networks which can lead to a 4 second delay in the establishment of calls to the EA (and with the information essential to the handling of the call potentially omitted).

These limitations may be cease to exist in the future and at which time Gamma will re-asses the viability of hosting numbers relating to EA’s on its network, however, in the meantime, we ask that our partners do not provision Gamma SIP or Horizon into any Emergency Authority.

Glossary

This appendix provides a basic glossary for some of the terms, acronyms, and abbreviations used in this document.

Term	Definition / Description
ADSL	Asymmetric Digital Subscriber Line
ANI	Automatic Number Identification
ASR	Answer Seizure Ratio

ATM	Asynchronous Transfer Mode
CAC	Call Admission Control
CDR	Call Detail Record
CLI	Calling Line Identity

CLIP	CLI Presentation
CLIR	CLI Restriction
CP	Communications Provider or Channel Partner.
CPE	Customer Premise Equipment
CPS	Calls per Second. The maximum number of new call attempts per second.
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTMF	Dual Tone Multi-Frequency
EDD	Ethernet Demarcation Device
G.711	ITU Recommendation for compounding digital audio
G.729	Audio data compression algorithm
GSP	Global Services Platform – Nortel TDM switch
GUI	Graphical User Interface
H.323	ITU-T VoIP Protocol
HA	High Availability
ISP	Internet Service Provider
IP	Internet Protocol (shorthand for TCP/IP)
IP DC	IP Direct Connect – Product name of the Gamma SIP Trunking service
IP PBX	IP Private Branch Exchange
IPT	Internet Telephony
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
LLU	Local Loop Unbundling
MOS	Mean Opinion Score
MSX	NexTone Multi-Protocol Session Exchange
NSN	National Significant Number
OSS	Operational Support Systems

PABX	Private Automatic Branch Exchange
PDD	Post-Dial Delay
POP	Point of Presence
PSTN	Public Switched Telephone Network
Q931	PABX signalling protocol (ITU definition)
RFC	Request For Comments
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol . A signalling protocol for Internet conferencing, telephony, presence, events notification and instant messaging.
SLA	Service Level Agreement
SME	Small/Medium Enterprise
SoHo	Small Office/Home Office
SQL	Structured Query Language
TSC	Gamma Technical Service Centre
TDM	Time Division Multiplexing (traditional digital telephony)
UDP	User Datagram Protocol
VoIP	Voice over IP
VPN	Virtual Private Network