Schedule 10 – SIP

Commencement date for provision of the Supplies

The date on which the Supplies become available for use by the Customer (regardless of whether or not they are actually used on that date), as specified in the first monthly invoice relating to the Supplies.

Description of the Supplies

The provision of SIP services, as described in this Schedule and specified in the Order Form.

Prices payable for the Supplies

As set out in the Order Form.

Service Level Agreements (SLAs)

A. Priority Levels

The following SLAs will apply to issue resolution provided that the issue falls within the Support Demarcation Boundary as defined below.

(a) *Priority 1, Critical Outage*

Problems that severely affect call processing service, traffic and require immediate corrective action (24x7) for example:

- 100% of users cannot access the Services;
- 100% of users cannot connect to voice servers;
- No inbound calls can be placed into the system;
- No outbound calls can be made from the system.

(b) Priority 2, Major Impact

Problems that cause conditions that significantly affect system operation, maintenance, and administration and require immediate attention. The urgency is less than in critical situations because of a lesser effect on system performance, for example:

- There are call processing issues with a majority group of users (>50% of users);
- The system performance is degraded;
- Administration of service is degraded;
- There is no reasonable workaround.

(c) Priority 3, Minor Impact

Problems which do not significantly impair the functioning of the system and do not significantly affect service to Customers, for example:

- Problem is non-critical or not service affecting;
- There is a reasonable workaround;
- Usability issue, documentation problem.

B. Priority Response Time Frames Definitions

B1. **Response:** the time from creation of a ticket until contacted by Connexus or its Relevant Subcontractor.

Resolution: the time from the creation of a ticket until Connexus or its Relevant Subcontractor have a full fix to the issue.

Level	**Category**	**Response**	**Target Fix**	**Measurement Period**
Priority 1	Critical	1 hour	4 clock hours	24 x 7 x 365
Priority 2	Major	1 hour	8 clock hours	24 x 7 x 365

Priority 3	Minor	4 hours	3 working days	Mon - Fri 0800 : 1800

B2. Connexus or its Relevant Subcontractor shall use reasonable endeavours to provide a solution within the above target timeframes. For Priority 1, Critical Outage and Priority 2, Major Impact issues, Connexus or its Relevant Subcontractor will aim to provide a temporary solution to temporarily fix the fault with the Service while a permanent solution is developed.

B3. Priority 1 issues may be downgraded to Priority 2, and Priority 2 issues may be downgraded to Priority 3, following the application of a temporary solution.

B4. To meet these goals, at the request of Connexus or its Relevant Subcontractor the Customer shall ensure that its personnel are on site and that remote access to the Service, or affected product or system is available to allow remote diagnostics and maintenance.

B5. The Service Levels shall only apply to faults traced to Connexus's or its Relevant Subcontractor's Service platform and not to Customer CPE and Customer network connectivity related faults.

B6. It is technically impracticable to provide a fault free Service and we do not undertake to do so

C. Incident / Fault Reporting

C1. To assist Connexus in meeting the service levels detailed in section B above, when reporting an issue, the Customer shall provide Connexus with:

(a) the date and time at which the problem occurred;
(b) the Service which the problem affected;
(c) the impact of the problem on the Service, including a detailed description of the issue, including:

- the components involved, and;
- the activity ID involved in the issue, and;
- any other information that Connexus may reasonably require.

C2. Following receipt of each new Incident, Connexus will allocate a unique Case Reference Number by the Connexus fault management system. The Customer and Connexus, at the time of making the incident/fault report, shall agree the priority level of the Incident in accordance with the criteria set out at section A above. Once opened, a support case will remain open until the Incident has been resolved.

D. Incident – Resolution Targets

D1. Connexus shall use reasonable endeavours to resolve an Incident within the timeframes defined in section B above. Such service is available 24 x 7 x 365 days per year for Priority 1 and Priority 2 incidents.

D.2. Repair times for non-Service affecting faults shall be agreed on a case-by-case basis. No service credits shall be payable for failure to repair non-Service affecting failures within the target repair time specified above.

E. Service Availability Targets and Levels

E1. The Service Availability target (defined below) relates to the ability of the Connexus-supplied SIP Trunks to be operational and in service as measured and determined by Connexus.

Service	**Monthly Availability Service Level**	**Service level triggering service credit**	**Service level triggering service credit**	**Service level triggering service credit**
		1st Trigger	2nd Trigger	3rd Trigger
SIP Trunking	99.95%	<99.95%	<98.0%	<95.0%

Service level triggering service credit	**The service credit as a percentage of the recurring monthly Charges for the affected Service shall be:**
1st Trigger	10%
2nd Trigger	30%
3rd Trigger	50%

E2. Downtime or unavailability relating to the following incidents shall not be treated as a period of unavailability in the Horizon or Avaya Hosted Telephony availability calculation, and the Horizon and Avaya Hosted Telephony and associated infrastructure and the Service shall be deemed to be available during any periods of downtime caused by any of the following:

(a) any matter beyond Connexus's reasonable control.

(b) Scheduled or Emergency Maintenance.

(c) any service affecting fault that is not classified by Connexus as a loss of service.

(d) the public internet (including without limitation any unavailability of the public Internet).

(e) the Customer requires an ancillary product.

(f) works carried out by anyone other than Connexus.

(g) failure by the Customer to provide prompt assistance and information, as requested by Connexus.

(h) any incident that is raised by the Customer that is subject to inaccurate or incomplete information.

(i) failure by the Customer to respond to an enquiry from Connexus or any third party acting on its behalf which delays, hinders or prevents Connexus from performing its obligations.

(j) Unavailability caused by a WAN or Internet service.

(k) Incidents, delays and failures by Connexus to meet any Service Levels which are caused by denial of service attacks.

F. Service Credits

F1. Except as otherwise provided in this Schedule, service credits are applied as follows:

Failure to meet the Service Availability target: If Connexus fails to achieve the Service Availability target set out in section E.1 above at any Site in any calendar month the Customer may claim service credits for the affected service.

F2. To claim a service credit, the following must be submitted to Connexus within 30 days from the date upon which the relevant Incident first occurred:

(a) The Connexus support case reference;

(b) The date and time of the first contact with Connexus;

(c) Sufficient evidence and information to describe and demonstrate to Connexus's satisfaction (acting reasonably) that an Incident has occurred and that such Incident was not caused by the Customer or end user, or any of the causes referred to in section E.2 of this Schedule; and

(d) A request for the applicable service credit.

F3. If the Customer fails to submit the above information and request to Connexus within such 30 day period, the Customer shall be deemed to have irrevocably waived its right to any service credit that would otherwise have been payable in respect of that Incident.

F4. Service credits can be claimed as discounts on the monthly charge. Note that for calculation purposes, a month is 43800 minutes long. Where there is no Monthly Committed Usage, service credits are calculated based on the method outlined above.

G. Exclusions

G1. In all cases, any periods during which Scheduled Maintenance and / or Emergency Maintenance is being carried out shall be excluded from any Service Level measurement periods.

G2. Incidents, delays and failures by Connexus to meet any Service Levels which are caused by denial of service attacks shall also be excluded from any Service Level measurement period.

H. Aggregate Service Credit Cap

Notwithstanding any other term of the Contract, in no event shall the service credits payable by Connexus in respect of a Service in any month exceed 100% of the Recurring Monthly Charges payable by the Customer in respect of that Service in that month.

Software licences

None.

Special Conditions

1. Definitions

The following definitions apply in this Schedule:

CLI: the call line identification number of the Customer when originating a telephone call.

Customer Order: an order for the supply of the Service and (where applicable) Equipment and / or Service Equipment.

Customer Order Variation: any variation to any Customer Order, including changes to any Service option, varying or adding to the Service or (where applicable) the supply of any additional or replacement Equipment and / or Service Equipment.

Relevant Subcontractor: the Subcontractor from whom Connexus is procuring and reselling the Service.

Relevant Subcontractor's Terms and Conditions: the terms and conditions of the Relevant Subcontractor for the Service as notified by Connexus to Customer.

Service: the Supplies more particularly described in this Schedule and the Order Form.

2. Provision of Service

2.1 Connexus shall be entitled to:

(a) change the technical specification of the Service (provided that such changes do not materially affect the performance of the Service) where necessary for operational reasons, statutory or regulatory requirements, as determined either by Connexus or the Relevant Subcontractor;
(b) suspend the Service for operational reasons or in case of emergency or in accordance with Condition 19 of the Conditions; and
(c) give the Customer instructions which Connexus or the Relevant Subcontractor believes to be necessary for health and safety reasons or for maintaining the quality of the Service.

2.2 Connexus shall use all reasonable endeavours to maintain the Service 24 hours in every day on every day of the year but shall not be liable for any failure to maintain the Service whether this arises from a technical or other failure of the telecommunications system used to provide the Service. Connexus does not warrant that the Service will be fault free or free of interruptions.

2.3 Customer Orders shall be subject to acceptance by Connexus and the Relevant Subcontractor. In the event of rejection by the Relevant Subcontractor after acceptance by Connexus, such acceptance shall be deemed to be of no effect.

2.4 Connexus will use its reasonable endeavours to ensure that all CLI data supplied correctly by the Customer, in accordance with the above provisions, will be processed within five days of receipt, provided that the Customer shall remain liable for all Charges for Services in the event that it takes longer than two days to deactivate such CLIs when requested to do so.

3. Orders for Service

3.1 Customer Orders and Customer Order Variations shall be subject to acceptance by Connexus.

3.2 Connexus agrees to set up the Service within reasonable timescales, subject to any timescales of the Relevant Subcontractor. All timescales and any provisional or proposed activation dates are estimates only.

3.3 The Service will commence on the activation date notified by Connexus, following completion of any required set-up and installation work.

3.4 Connexus reserves the right to revoke its acceptance of any Customer Order or Customer Order Variation, if for any reason a Service connection cannot be provided to any relevant Customer premises having regard to any geographic, practical or technical issues arising.

This may not be discovered until the last minute when an attempt is made to set up the Service.

3.5 Termination of the Service will take effect at the end of the month following the month in which the Customer gives notice of cancellation.

4. Variation to the Service

4.1 Connexus shall be entitled to make variations and additions to the Services from time to time (acting reasonably) including:

(a) to improve or add to the Services;
(b) to make changes for operational reasons where these do not have a materially adverse effect on the Services;
(c) to pass through any change made by the Relevant Subcontractor;
(d) in order to comply with any law or legal obligation (whether under common law, statute, tort or otherwise), or any change to any law or legal obligation;
(e) in order to comply with any final order, provisional order, direction, notice, specification, designation or consent made by the Office of Communications; and
(f) in order to maintain the integrity or security of the Services and / or any part of Connexus's or the Relevant Subcontractor's systems.

5. Customer obligations

Any Customer equipment connected to or used with the Service must be connected and used in accordance with any instructions, safety and security procedures applicable to the use of the equipment. Any equipment, which is attached (directly or indirectly) to the Service must be technically compatible with the Service and approved for the purpose under any relevant legislation or telecommunications industry standards.

6. Usage conditions

6.1 In addition to the Contract, the Customer acknowledges and agrees that the Relevant Subcontractor's Terms and Conditions shall apply to the Service.

6.2 Use of the Service is subject to Connexus's acceptable use policy published from time to time and the Customer must not use the Service in any way that in Connexus's reasonable opinion could or does detrimentally the performance of Connexus's systems or network or those of any Relevant Subcontractor, or detrimentally affect the quality of the Service to any other customers. Connexus reserves the right to take appropriate action in such circumstances.

6.3 All applicable laws and legal obligations must be complied with in connection with any use of the Service, including in relation to any activity or occupation carried out through or using the Service, and including in relation to any data, information or other materials hosted, transmitted or otherwise processed using the Service.

6.4 In particular, the Service shall not be used:

(a) for or in connection with any activity which would be criminal, fraudulent or otherwise unlawful under any applicable law;
(b) to make, send, knowingly receive, upload, download, or process any data, information, message or other communication (whether data or voice), or other material which is immoral, offensive, abusive, indecent, defamatory, obscene or menacing, improper, or may cause annoyance, inconvenience or needless anxiety, or is in breach of any copyright, confidentiality obligation, or any other intellectual property right; and / or
(c) to spam or otherwise to send or procure the sending of any unsolicited advertising or promotional material, unless permitted by law, or knowingly to receive responses to any spam, unsolicited advertising or promotional material.

6.5 Where, acting reasonably, Connexus or the Relevant Subcontractor considers that any Service is being used in breach of these usage conditions, or Connexus or the Relevant Subcontractor considers that any use being made of the Service may cause Connexus or the Relevant Subcontractor to incur any legal liability or to commit any offence, then Connexus or the Relevant Subcontractor may temporarily suspend such Service. Connexus will endeavour to give 4 days' notice of such action, unless shorter notice or no notice is justified in the circumstances.

6.6 Connexus will only be obliged to re-instate the Service if Connexus is reasonably satisfied that no breach has occurred or will continue and that no liability will be incurred or offence will be committed by Connexus or the Relevant Subcontractor.

6.7 The Customer shall co-operate in any such investigation, and the charges for the Service will continue to be payable during such period of suspension.

6.8 The Customer shall indemnify Connexus against any liability Connexus may incur as a result of any breach of the above conditions, including any liability of Connexus under a like indemnity to the Relevant Subcontractor. The limitations and exclusions of liability contained in the Condition headed “Limitation of Liability” in the General Terms and Conditions do not apply to this indemnity. The liability arising out of this indemnity is limited to £1 million for any one event or series of connected events and £2 million for all events (connected or unconnected) in any period of 12 calendar months. Connexus shall have a duty to mitigate its loss in the circumstances covered by this indemnity.

Service Overview

The Service provides VoIP connectivity for certified PBX's, allowing inbound and outbound telephony through the network for termination with both national and international destinations.

The 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.

The Connexus 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 Connexus’s network. However, it should be noted that the features are not guaranteed to be supported on every platform connected to the Connexus SIP Trunk Service because of vendor interoperability issues.

The SIP Trunk Service provides SIP signalling as a method for customers to inter-connect with Connexus’s VoIP network supporting calls to / from the PSTN as well as VoIP to VoIP calling between SIP accounts created within the 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, 123 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 Schedule.

Customers can access the Connexus SIP Trunk Service via public internet or private interconnects. These connectivity options include the following:

- Private and Public connections not provided by Connexus;
- 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.

Connexus offers three design options as standard, for the configuration of the Customer’s Connexus SIP Trunk Service:

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

Service Features

Connexus SIP Service supports Network Number CLI presentation and Privacy definitions in accordance to RFCs 3323 and 3325, using P-Asserted ID and Privacy Headers only. Connexus requires Customers to supply the PAID and, where required, the Privacy Headers. Connexus does not support the use of the invalid statute Remote Party ID (RPID) definitions and such Headers will be removed.

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 Connexus's network presents a geographic number in the UK National format, Connexus's 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 Connexus provided Geographic Number that is allocated to the Endpoint at order creation;
- A Connexus 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 our Network;
- The A-number is checked against a database on our network of geographic numbers that are allocated to the Connexus 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 allocated Geographic DDI range. This default CLI can be changed if required.

Connexus 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 carrier's 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 Connexus allocated account range, rather than the intended CLI for presentation. Connexus are 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.

2. Calling Line Restriction (CLIR)

When the calling (A-Party) has requested privacy (CLIR), Connexus will enforce privacy in accordance with RFC3325. Calling party information, including From Address, Contact and associated Privacy Header (PAID) are withheld from an endpoint.

3. Call Park, Transfer and Conferencing

The Connexus SIP Trunk Service provides the features listed below in the majority of cases but they 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.

4. Emergency Call Divert

The Connexus 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, Connexus can activate either all pre-configured numbers with a single action, or activate individual diverts as necessary. Once activated, these diverts become effective.

- Deactivation is performed in the same manner as activation.
- 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.
- Connexus 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 enabled within Connexus's supplier's 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.

5. Fraud Alert

Connexus 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 24 hour and 7 day periods with individual figures associated with both. On reaching 85% of the maximum spend in any period, the Customer will receive a call and an email alerting them to the fact. If the spend reaches 100% of the agreed limit the Customer will receive a further call and an email and all subsequent calls from that end-point will be barred.

Service can be restored by the Connexus 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.

6. CLI Flexibility

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

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 the Service being suspended and / or withdrawing the use of the Presentation CLI Flexible Service.

For calls made to the Emergency, Non-emergency & Operator Services (100, 101,111,112,116, 118,123,1800 and 999), only Connexus 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 DDI range allocated to the Customer.

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 Connexus 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 Connexus's network.
- Maximum Egress Calls – specifies the maximum number of calls that may be placed to that endpoint by Connexus's network.
- For example, if the channel limits is 100 concurrent calls, and there are 70 ingress calls, the maximum number of egress calls allowed will be 30.

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

8. Call Barring

By default, calls to international and premium numbers will be barred. Customer profiles can be modified so that their profiles allow or restrict access to:

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

Similarly, the Customer's barring profile can be modified to allow or restrict all outbound and / or inbound calls. Calls to the emergency services 999, 112 remain unaffected irrespective of the barring applied.

9. Fax and DTMF Support

The Connexus 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.

Due to different vendor implementations Connexus 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.

10. Emergency, Non-emergency and other short code calls

Important Note: Connexus provides 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 Connexus, so that the emergency services operator will check the address details on the National Database. It is the Customer’s responsibility to ensure that the address associated with the default site CLI is always up to date. Connexus will maintain these addresses as advised by the Customer.

Ofcom expect that any calls originating on the Connexus 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 a Customer’s account has been suspended.

In such circumstances the 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.

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).

<u>Service Characteristics</u>

1. Endpoints

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

2. Maximum Calls Per Second (CPS)

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

Account type	**Calls/second limit**
Single endpoint design	2
Resilient endpoint design	5

If this constraint is reached, calls will be logged and rejected with a SIP response 486.

3. 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 ˜ 10 usable concurrent channels available. The figures for VoIP using ADSL access are similar.

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

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

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. Long Duration Calls

Connexus’s supplier has a policy of terminating any call that exceeds eight hours,

5. IP Addressing

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

6. 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 Connexus’s supplier controls the sample period in both the egress and ingress directions of calls made by its customers. Connexus support G.729-A only as a G.729 variant, no other variants of this codec are supported.

Connexus’s supplier does 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.

Connexus’s supplier polices the media-stream bandwidth based on the negotiated codec. If a Customer 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. Support for Silence Suppression and Comfort noise is available to Microsoft Lync connections only.

Ptime. There is no support for the negotiation of codec Ptime. One of the two supported voice sample periods must be selected for the desired codec, so eradicating the need for Ptime negotiation. This Customer-selected sample period results in a Ptime which is policed by Connexus’s supplier.

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

7. Session Failover and Endpoint Resilience

The following scenarios will result in an endpoint 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 Ping failure (depending on build type, see below for details);
- SIP failure response code;
- CAC exhaustion (depending on build type, see paragraph 7 of the section headed “Service Features” above for details).

Destination unreachable

This happens in two ways:

- An ICMP unreachable message is received 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 re-transmitted 3 times. If that limit is reached, the Network will stop trying that endpoint and initiate failover to another endpoint.

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

SIP Ping failure

If SIP Ping is enabled at both the SBC and the endpoint and SIP Ping fails to respond favourably. SIP Pings are sent every 60 seconds. The Customer's CPE should reply with a 200 OK.

If a response is not received within 3 pings, the endpoint is removed from service after the 3rd unsuccessful response. SIP Pings will continue to be sent out every 60 seconds and as soon as 3 responses are received the endpoint will be brought back into service.

Please note that depending upon build type, the response to a SIP Ping failure may be a non-huntable 486 (Singleton, Enhanced, Active/Standby, Resilience+) or a huntable 503 (Loadshare). It is therefore advisable that SIP Ping not be used on build types other than Loadshare.

SIP Response Codes

When a SIP Final Response is received, code as detailed in Table 11, in reply to 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 Customer's network (Proxies and CPE) session timers, as specified by RFC 4028 are implemented. The preferred method 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 Session-Expires 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. 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.

8. Customer Premises Equipment

The supply, provisioning and support of all Connexus-supplied hardware at the Customer's site is the responsibility of Connexus.

Important Note:

If connection is required for a Customer device that has not previously been connected to the network, Connexus can request its supplier's cooperation with conformance testing to ensure that the device is fully compatible with the network prior to live provisioning with a Customer.

9. Network Security

Access to the SIP Trunk Service from the Customer's 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**).

Customer Network Design Options

Three basic design options are offered as standard for the Connexus SIP Trunk Service:

- Single Site – A single site working off a single 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 SBC HA Clusters. This enhanced Service offers multiple Customer IP addresses and the 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 SBC HA Clusters. This enhanced Service offers multiple Customer IP addresses and the 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. There are limits to the number of SBC's and Endpoints that can be added to a resilient configuration, Customers should contact Connexus to discuss larger configurations than the standard.

Network Access and Connectivity Options

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

- *Public internet.* The Customer's CPE (typically an IPBX supporting SIP) is defined as an 'endpoint' within the 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 authenticate the endpoint, providing duplex interconnection to the PSTN.
- *Private interconnect*. In order to assuage perceived security and quality concerns, the following access options are offered:
  - Private interconnection via the Connexus IP Assured service;
  - Private interconnection via Ethernet;
  - Private interconnection to into the POP (Layer 2 VLAN) .

IP Addressing and Connexus Ethernet connectivity

For SIP Trunking Customers connecting via Connexus Ethernet, a private /29 subnet is allocated for use on the Customer side of the Connexus supplied 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.

Fraud Management Service Description

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

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

1. Functionality Overview

The system monitors the Customer's spend by systematically polling call records and rating them accordingly. The accumulated total from the notional start time (i.e. when monitoring 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 to Connexus.

Connexus can then choose to take some form of action, investigating with the Customer 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 24 hour 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 notes 1,2 and 3 below).

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 over-run 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.

2. Terms and conditions

If an endpoint had the Fraud Management System (**FMS**) feature set enabled, it will be applied and charged to all channels on the endpoint.

Connexus will only waive charges for calls that breach the configured threshold (see note 2 above) where they can be shown 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 Customer in all circumstances. Connexus reserves 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 Terms and Conditions. In the event of a conflict with the Contract the above terms and conditions shall apply.

3. Configuration

Daily Spend Limit

The daily spend limit is a rolling 24 hour 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 hour 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 beached detailing the following:

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

A warning email will also be sent prior to call barring if the threshold alert warning has been configured.

Resetting after breach

Connexus will remove call blocking from an endpoint following automated call barring.

Connexus can also choose to modify the spend limits accordingly.

<u>Dialler Policy</u>

No Dialler traffic is permitted on the SIP trunking service, such traffic will be removed if / when detected.

Please be aware that all SIP traffic is actively monitored, and action will be taken on 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 Connexus from barring the endpoint without notification in extreme circumstances.

<u>Provisioning</u>

Please contact the Connexus Service Team for SIP Provisioning, In Life Changes and lead times.

<u>Billing</u>

Please call or e-mail the Connexus Billing Department for SIP Trunk Service related billing queries.

t: 01453 827700 (Opt 2)

e: accounts@connexusuk.com.

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.

Connexus 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 cease to exist in the future and at which time Connexus’s supplier will re-asses the viability of hosting numbers relating to EA’s on its network.