Service Description

Modern Comms Managed Service – Advanced

November 2025

transparity

Contents

1. Service Overview

The Modern Comms Managed Service Advanced includes support, monitoring and a range of proactive services for session border controllers (SBC), Microsoft Teams and Dynamics Contact Centre based solutions.

2. Service Features

The following is a high-level overview of the functionality available within this service:

KEY:

● Inclusive as part of the standard service offering

◒ Inclusive and as standard when you have purchased the relevant service or if you have requested service(s) that have been documented in your SoW.

○ Available as an optional upgrade for an additional fee.

Feature	Advanced
24*7 Incident Response	●
SBC Platform Monitoring and Maintenance	●
SBC Failover Testing	●
SIP Infrastructure Management	●
Service Requests	●
Customer Success Architect incl. Best Practice Reviews	●
Service Management	●

2.1 24*7 Incident Response

For incidents within your SBC, Microsoft Teams, or Microsoft Teams Meeting Rooms environment we will provide 24*7 incident response, if the Incident relates to the services provided by a 3rd party provider including Microsoft, AudioCodes and Gamma, we will escalate and manage the escalation.

We will follow the Target Response as defined in section 8.1 of this service description.

2.2 SBC Platform Monitoring and Maintenance

We will provide ongoing proactive monitoring of your SBC's utilising the One Voice Operations Centre (OVOC), including the following: -

- Streamline Session Border Controller management and quality monitoring
- Real-time call quality monitoring and root cause analysis
- Increased efficiency with centralised configuration, provisioning and license management
- Intelligent insights into network trends, voice quality and performance through self-service reports
- Centralised reporting

The OVOC service is hosted and used by Transparity in the course of providing support. Integration will be configured as a part of the SBC deployment.

As a component of the Managed Service, firmware updates (where available) will be applied once every six (6) months outside of core business hours. Following installation, full testing will be completed along with the updating of related support documentation.

2.3 SBC Failover Testing

Transparity will carry out formal failover testing at least once every six (6) months to ensure service continuity in the event of hardware or component failure. Test steps will be defined at the point of service initation and documented in a failover plan. This document will be reviewed and maintained following each test along with test records to validate the success / failure of each test occasion.

2.4 SIP Infrastructure Management

As part of this service, we will manage your SIP infrastructure including the following activities: -

- Proactive monitoring of SIP traffic and call quality
- SIP registration and authentication management
- Provisioning and configuration of SIP trunks (through service requests)
- Capacity and scaling management

2.5 Service Requests

The managed service includes up to five (5) service requests per month for configuration and non-incident related changes to the supported systems.

A list of included service requests items is available on request.

2.6 Customer Success Architect

You will be assigned a dedicated Customer Success Architect (CSA). The CSA will be an experienced technical consultant or architect with expertise across the Microsoft portfolio.

You will have direct access to your CSA for anything that isn't time sensitive or mission critical such as:

- Expert Consultation: Receive answers to your technical questions from an expert, helping you navigate the complexities of the SBC, Microsoft Teams or Dynamics Contact Centre
- Strategic Guidance: Benefit from strategic advice and best practices to optimise your environment, improve performance, and reduce costs.
- Best Practice & Feature Review: In life reviews of your SBC and Microsoft Teams configuration to ensure alignment with industry best practice and new features and functionality.

2.7 Service Management

As part of your account team, you will be allocated a Customer Success Manager. They will serve as your primary contact(s) for day-to-day management and interaction for this Service. In addition, the Customer Success Manager will act on your behalf to ensure we adhere to our processes and standards to meet contracted obligations and provide advice and guidance on your environment.

The responsibilities and/or deliverables of your allocated Customer Success Manager will include the following as outlined in the table below: -

Name	Description	Frequency	Forum
Operational Risk Management and Tracking	An operational repository (including the Risk Register) will be created for all risks identified and will include information about each risk, e.g., the	Quarterly	Service Review

Name	Description	Frequency	Forum
	nature of the risk, reference, and owner, as well as any mitigation measures. This report will be reviewed with you via Customer Success Manager at your service reviews.		
Continual Service Improvement Advice	Strategic advice based on intelligence provided by the Service to investigate how we can potentially increase the quality of products and services at a minimal cost for you. This advice will be tracked in a Continuous Service Improvement plan owned by the Customer Success Manager. This will be reviewed with you via Customer Success Manager at your agreed service reviews.	Quarterly	Service Review
Utilisation Report	Quarterly review of the SIP utilisation	Quarterly	Service Review
SLA Breach and Complaints Management	We provide support including graphical information and narrative to you.	As and when an Incident occurs	Service Review
Risk Register	We maintain a register of all known risks for ongoing management – please refer to the Operational Risk and Management Tracking above.	As and when a risk occurs	Service Review

3. Service Operations

Please refer to our Operations Manual for further information on incident management, requests for change and information requests.

4. Billing

4.1 Additional Charges

We reserve the right to charge additional fees in the following situations:

- Implementation work carried out outside Business Hours; and
- Any change in your requirements occurring after the implementation of the Service and outside the scope of the contract (as described in the MSA).

5. Dependencies

We will provide the service subject to the following dependencies:

- All professional services required to set up this Service will be subject to separate Statements of Work (SoW) and Charges and, where applicable, Service Descriptions.

5.1 Customer Obligations

- You will provide us reasonable assistance in the performance of the Service(s) including, but not limited to, providing all technical and licence information that we may require to perform the Service(s).
- You will provide named contacts who will be authorised to submit support requests on behalf of your company ("Nominated Contacts"). They will be the designated people with whom all contact is made regarding all requests.
- You will provide us with access to the in-scope subscriptions, accounts, and tenants. This access will be used by our support staff and tooling. For example:
  - Microsoft's Partner Admin Link (PAL);
  - Microsoft Granular Delegated Access Permissions (GDAP) relationship;
  - Microsoft 365 Lighthouse relationship and delegations;
  - Service Principals;
  - Administration break-glass accounts; and
- For Microsoft 365 subscriptions not purchased through our CSP we will not be able to raise incidents with Microsoft unless you have purchased a separate Microsoft support agreement;
- You will allow us to deploy infrastructure in each public cloud region to handle the collection of activity and diagnostics logs into our monitoring platform.
- You will actively work with our operations team to resolve any raised incidents or Service Requests, or any activities relating to patching, that require your input or action. For example, you may be required to make any required changes to an end user device to which we have no access.
- Some incidents may require user-impacting remediation activity. You are responsible for distributing and coordinating end-user communications and activity unless agreed otherwise during the planning of the activity.
- It is your responsibility to comply with your data sovereignty controls, policies, and procedures.
- Customers are required to maintain an active support agreement with AudioCodes for the purpose of incident escalation. This will be represented in the cost of the service where licensing is procured via Transparity.
- Should session quantities require increase within the contact term a revised version of this agreement will be presented to reflect changes to pricing and the contract period.
- AudioCodes will provide Transparity with business hours support for issues and failures of the Session Border Controller. Customers can record high priority incidents on a 24/7 basis; however, vendor progression will only be possible within the hours specified within the vendor support agreement. Options will be presented within your Sales proposal.
- You agree to proactively support the collation and maintenance of pre-requisite information required to deliver the Managed Support Service (e.g. system documentation, network diagrams, administration accounts etc.).
- You acknowledge that the provision of the Managed Services does not guarantee that an incident will not take place. We will not accept liability for any incident except where it is the result of Our negligence in the provision of the Session Border Controller Managed Service (and only then to the limit set out within Our Terms and Conditions).
- All configuration changes should be made in tandem with Transparity, ensuring qualification of changes and the ability for an up-to-date copy of the running configuration to be held securely on file.
- The Managed Services detailed within this document apply to a Direct Routing solution. Unless explicitly specified, the support of other products and services related to the delivery of the solution are out of scope (e.g. endpoint devices, Microsoft Teams, Microsoft 365 etc.).
- You agree to the installation of monitoring agents on in-scope devices and the deployment of the Audiocodes One Voice Operations Centre monitoring solution. These services will gather and send performance and telemetry data to support systems used by Transparity in the provision of the service.

- Changes are restricted to those that are estimated to take less than 2 hours and where the risk can be appropriately managed remotely. Changes which require significant reconfiguration of the Session Border Controller or those which introduce significant risk based on the opinion of Transparity are not included within the scope of this Managed Service. Such changes will be highlighted at the earliest opportunity and referred to your Account Manager for formal scoping.
- The implementation of changes not explicitly referenced in-scope is not included and will be subject to standard proposal and project deployment activity (which may be deducted from a Timebank, where applicable).
- We reserve the right to defer or reschedule any planned changes in the event a Critical Incident investigation prevents this. Critical Incident Response will always take priority over Monitoring Alerts and tasks that can be deferred.
- We will collect and store information relating to the designated support contacts within our Incident Management system (Autotask). You agree to the collection of this data which will include (but may not be limited to) names, email addresses, locations, contact telephone numbers, and IP addresses.
- By adopting the Managed Support Service, you agree to empower us to remediate in incidents on your behalf in accordance with our Service Desk procedures. We will endeavour to highlight and mitigate any impact to your organisation. However unforeseen issues can occur, and you agree to work with us to resolve these issues if required. Transparity operate a “fix forward” approach to consequential issues but will fail back if required.
- If emergency remediation is required, we will seek approval from you before proceeding. However, if no response is received in a timely manner, then we reserve the right to implement remedial actions even if they are impactful to your organisation. We will assist with any ramifications after the fact. We will notify you of any remedial actions via email or ticket updates.
- Identified risks will be logged into our risk register. We will always seek to work with you on these risks and have you approve them where you do not wish or are not able to remediate the item. If we are unable to contact you in a timely manner or if you delay approval of the risk, the risk will be logged and automatically approved on your behalf. These open risks will form part of the ongoing monthly report for you to review.
- In certain circumstances we may determine that the most rapid route to recovery is the redeployment of your Session Border Controller appliance. In this situation we will deploy a fresh appliance and apply the most recent configuration backup on file.
- Should a failover test fail, the root cause together with remedial recommendations will be presented to you by your Service Delivery Manager. Until these recommendations are implemented you accept that the ability to failover will be impaired. Transparity will not accept responsibility for the loss of any data / systems caused in response.
- Additional costs relating to the running of your Session Border Controller in Azure will apply. An indication of additional licensing required will be provided in Your sales proposal, however due to the consumption nature of Cloud services these prices may vary over the course of the Service Term.
- In the event that you fail to adopt recommendations or progress active risk register items raised during the execution of the service our ability to provide the service may be diminished. Should this lead to a material reduction in the quality of the service we can provide, we reserve the right to terminate the Managed Support Service. Your Service Delivery Manager will highlight and seek to progress issues falling into this category; liaising with you and your Account Manager to identify and communicate corrective actions necessary to maintain the service before such action is taken.

5.2 Service Restrictions

- We will provide and support the Service on a reasonable endeavours basis only and will not be subject to any availability targets, if:
  - the OS residing on your end user device is out of vendor support, or
  - no support contract with the OS provider is in place, or

    - the end user device is configured in direct contravention of the requirements, best practices, or specific guidelines for support.
- When a ticket is opened with a 3rd party vendor the Transparity SLA is paused until a response is received from the 3rd party vendor
- We reserve the right to defer or reschedule any planned changes in the event a Critical Incident investigation prevents this. Critical Incident Response will always take priority over Monitoring Alerts and tasks that can be deferred.

6. Exclusions

- The implementation or configuration of new technology is not included within the Modern Comms Advanced Managed Service. Where this applies your Account Manager will present our recommended approach in a costed proposal for your approval
- Identified risks will be logged into our risk register. We will always seek to work with you on these risks and have you approve them where you do not wish or are not able to remediate the item. If we are unable to contact you in a timely manner or if you delay approval of the risk, the risk will be logged and automatically approved on your behalf. These open risks will form part of the ongoing monthly report for you to review.
- In the event that you fail to adopt recommendations or progress active risk register items raised during the execution of the service our ability to provide the service may be diminished. Should this lead to a material reduction in the quality of the service we can provide, we reserve the right to terminate the Modern Comms Advanced Managed Service. Your Customer Success Manager will highlight and seek to progress issues falling into this category; liaising with you and your Account Manager to identify and communicate corrective actions necessary to maintain the service before such action is taken.

6.1 Third Party Related

Certificate management is limited to server endpoints and platform services. Certificate renewals or management on end user devices is not in scope.

7. Definitions and Acronyms

In this document “we” or “us” refers to the Supplier, and “you” refers to the Client.

7.1 Terms

The terms listed have the following meanings:

Term	Meaning
Statement of Work	This means a document that defines project-specific or Customer-specific activities, deliverables, and/or timelines for providing services to that Customer.

7.2 Acronyms

Acronym	Meaning
CSP	Cloud Solution provider
GDAP	Granular Delegated Access Permissions
OS	Operating System
PAL	Partner Admin Link

Acronym	Meaning
PaaS	Platform as a Service
SBC	Session Border Controller
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SoW	Statement of Work
VM	Virtual Machine
VPN	Virtual Private Network
WAR	Well Architected Review

8. Service Level Agreement and Operational Targets

8.1 24*7 Incident Response

	P1	P2	P3	P4	P5
Hours of Support	24*7 Mon – Sun	24*7 Mon – Sun	08:00-18:00 Mon – Fri	08:00-18:00 Mon – Fri	08:00-18:00 Mon – Fri
Response	15 mins	Four (4) hours	Eight (8) hours	Twelve (12) hours	Twenty-Four (24) hours

8.2 Incident Prioritisation

Priority	Severity	Description
P1	Critical	**Business service outage** • System/Service/Application down or unhealthy. Extremely urgent • Very high impact in all business areas, extreme impact on multiple users and disruption is excessive, such as Cloud platform failures, Virtual Machine failures and Cloud networking or connectivity failure • Business critical - work cannot continue
P2	High	**Business service impaired** • High impact on significant business areas or specific users • Individual user cannot complete high priority/business-critical work, or department or group of users unable to continue with routine work • Business critical - work is impaired
P3	Medium	**Group of users affected** • Platform or application problem – user or group priority work cannot be completed • A group of users are experiencing system or business application
P4	Low	**One (1) person affected or minor service fault** • Minor system or application error • Backup or Patching Failure • An individual user is experiencing system or business application problems but is still able to work
P5	Routine	**Non-urgent investigations** • General advice and guidance or agreed scheduled activity